İnsan ve Toplum Bilimleri Araştırmaları Dergisi
Journal of the Human and Social Science Researches
[2147-1185]
12 th Years

2023, 12 (1), 393-418 | Araştırma Makalesi

Elektronik Posta Sistemine Üçüncü Taraf Güveni Gerektirmeyen Bir Çözüm Önerisi

Mansur BEŞTAŞ [1]

Öz

Bireyler ve kurumlar arasında bilgi ve belgenin iletilmesi, günlük hayatın olağan süreçlerinden biridir. Ancak bilgi ve belgenin güvenli olarak iletilmesi günümüzde önemli problemlerden biridir. Bilgi ve belgenin aktarımı noktasında, uzunca bir süre elden teslim, posta ve ilan gibi fiziksel yöntemler tercih edilmiştir.Günümüz dünyasında teknolojinin gelişimi ve internetin hayatın önemli bir kısmına sirayet etmesiyle birlikte, iletişimde önemli gelişmelerin oluşmasına neden olmakla birlikte bu etkileşim ve iletişim süreçlerinde elektronik yöntemlerin çeşitliliğini de beraberinde getirmiştir. Etkileşim ve iletişimde yoğun bir şekilde kullanılan elektronik sistemler sayesinde internet teknolojisindeki hız, verimlilik artışı ve maliyetlerin düşmesi de sağlanmıştır.İnternet teknolojilerinin sağladığı imkânlar vasıtasıyla elektronik posta ortaya çıkmıştır. Elektronik posta kullanıcılarının kayıt altına alınması ile kayıtlı elektronik posta sistemi oluşmuştur. Kayıtlı elektronik posta sistemi, genel olarak elektronik postayı gönderen ve gönderiyi alan arasında var olan iletişimin belli standartlarda gerçekleştirilmesi sonucunda yasal kanıtların oluşturulması esasına dayanmaktadır. Böylelikle yasal altyapısı olan ve güvenliği arttırılmış olan bilgi ve belge aktarım yöntemi elde edilmiştir. Kayıtlı elektronik posta sistemi yasal standartlar ile belli bir seviyede güvenlik sağlamaktadır ancak merkezi mimariye sahip olarak tasarlanmıştır. Merkezi mimariye sahip çözümler, doğası gereği merkezi yapının güvenliği üzerine kuruludur. Bu güven kendi içinde de problemler içermektedir. Ancak merkezi yapıya alternatif olarak merkezi olmayan ve üçüncü tarafa güven gerektirmeden verinin yönetilebildiği yöntemler bulunmaktadır. Bu yöntemler içerisinde en yaygın olarak kullanılan yöntem blok zincir teknolojisidir. Blok zincir teknolojisi verinin yönetilmesi alanında yenilikçi bir yöntem sunmaktadır. Blok zincir teknolojisinin veri yönetimi açısından sunduğu yenilikçi bakış açısı ve sağladığı faydalar nedeniyle günlük hayatta veri yönetimi ile ilgili birçok uygulama tercih edilmeye başlanmıştır. Çalışmada, kayıtlı elektronik posta sisteminin merkezi mimarisine alternatif olarak blok zincir teknoloji kullanımı önerilmiş olup blok zincir teknolojisine entegrasyonu açıklanmıştır. Bu çalışmada amaç; blok zincir teknolojisinin kullanımının kayıtlı elektronik posta sisteminde uygulanması ve merkezi yapıda olan benzeri süreçlerin ve yazılımların güvene dayalı olan güvenlik zayıflıklarının ortadan kaldırılmasına yönelik çözüm önerisi ortaya koymaktır. Çalışma, elektronik posta sisteminin blok zincir teknolojisi ile yeniden tasarlanması ve entegrasyonunun detaylandırması açısından özgün bir çalışmadır. Bu çalışmada öncelikle kayıtlı elektronik posta sisteminin kavramsal çerçevesi hakkında bilgi verilmiştir. Ardından kayıtlı elektronik posta sisteminin temelini oluşturan yasal altyapı açıklanmıştır. Kayıtlı elektronik posta sisteminin kullanımının bireyler ve kurumlar açısından faydalarına değinilmiştir.

Anahtar Kelimeler: Blokzincir, KEP, Kayıtlı E-posta Sistemi , Elektronik, Güven.

Beştaş, M. (2023). Elektronik Posta Sistemine Üçüncü Taraf Güveni Gerektirmeyen Bir Çözüm Önerisi . *İnsan ve Toplum Bilimleri Araştırmaları Dergisi* , 12 (1) , 393-418 . https://doi.org/10.15869/itobiad.1168547

Geliş Tarihi	30.08.2022
Kabul Tarihi	29.03.2023
Yayın Tarihi	29.03.2023
*Bu **CC BY-NC** lisansı altında açık erişimli bir makaledir.

[1] Dr, Siirt Üniversitesi , Türkiye, mansur@siirt.edu.tr / ORCID: 0000-0002-8192-2044

İnsan ve Toplum Bilimleri Araştırmaları Dergisi
Journal of the Human and Social Science Researches
[2147-1185]
12 th Years

2023, 12 (1), 393-418 | Research Article

A Solution Proposal That Does Not Require Third-Party Trust in the Registered Email System

Mansur BEŞTAŞ [1]

Abstract

The exchange of information and documents between individuals and institutions is a common occurrence in everyday life. However, one of the major issues is the secure transmission of information and documents. For the transfer of information and documents, physical methods such as hand delivery, postal service, and public announcement have long been preferred.Communication has advanced significantly due to the development of the Internet, and electronic methods are now used in the field of communication. The use of internet technologies has provided and improved the benefits of communication speed, efficiency, and cost reduction.Through the possibilities provided by internet technologies, electronic mail technology has emerged. A registered e-mail system was invented with the registration of e-mail users through legal authorities. The registered e-mail system is generally based on the creation of legal evidence as a result of solid standards communication between the sender and the receiver of the e-mail. As a result, an information and document transfer method with legal infrastructure and increased security has been obtained. The registered e-mail system meets legal standards for security, but it is designed with a centralized architecture. Trust in the centralized structure is inherent in solutions with a centralized architecture. This trust has its own issues.However, as an alternative to the centralized structure, there are decentralized methods that can be managed without the involvement of third parties. Blockchain technology is the most widely used of these methods. Blockchain technology provides a novel approach to data management. Because of the innovative viewpoint and benefits that blockchain technology provides in terms of data management, it has begun to be preferred in many applications related to data management in everyday life. The study proposes and explains the use of blockchain technology as an alternative to the central architecture of the registered electronic mail system.The purpose of this research is to implement blockchain technology in the registered e-mail system and to propose a solution to eliminate the security flaws of similar centralized processes and software. The study is unique in that it redesigns the electronic mail system and elaborates on its integration using blockchain technology.The conceptual framework of the registered e-mail system is presented first in this study. The legal infrastructure that underpins the registered e-mail system is then explained.

Keywords: Blockchain, Registered E-mail Address, Certified Electronic Mail, Electronic.

Beştaş, M. (2023). A Solution Proposal That Does Not Require Third-Party Trust in the Registered Email System . *Journal of the Human and Social Science Researches* , 12 (1) , 393-418 . https://doi.org/10.15869/itobiad.1168547

Date of Submission	30.08.2022
Date of Acceptance	29.03.2023
Date of Publication	29.03.2023
*This is an open access article under the **CC BY-NC** license.

[1] PhD, Siirt University , Türkiye , mansur@siirt.edu.tr / ORCID: 0000-0002-8192-2044

Giriş

Kamusal yaşam, bu yüzyılda bilişimin gelişimi ve buna bağlı teknolojiler açısından iletişimin hız kazanması ve verimliğin arttırılması yönüyle pozitif yönde etkilenmiştir. İnternet teknolojileri ve buna bağlı iletişim teknolojilerinin gelişimi, bireysel ve kurumsal boyutuyla bilgi ve belge paylaşımının en önemli destekleyici unsurlarından biri olmaktadır. Günümüzde teknolojik imkânların yaygınlaşması ve kullanımı sonucunda fiziksel sınırlar önemini kaybetmeye başlamış ve fiziksel sınırların kısıtlılığı dikkate alınmadan iletişim gerçekleştirilebilmektedir. Fiziksel sınırların, iletişim açısından öneminin azalması küreselleşmenin her anlamda hız kazanmasını sağlamaktadır. (Organ ve Karadağ, 2011, s.82).

Teknolojik gelişmeler, sadece fiziksel sınırları değil ayrıca zaman kavramını da farklı bir boyuta taşımıştır. Teknolojinin etkilediği iletişim yöntemleri, bireylerin hayatında kendine yer bulmuştur. Bununla birlikte kamu hizmetlerinin geliştirilmesi bakımından ilk kullanım örnekleri ortaya çıkmıştır. Kamusal hizmetlerde bilişim teknolojileri ve bağlı iletişim teknolojisinin kullanımına yönelik ilk çalışma örnekleri 1990'lı yıllarda görülmeye başlanmıştır. Türkiye'de, elektronik temelli devlet uygulamalarının ortaya çıkışı 2000'li yıllara dayanmaktadır (Yüce ve Çelik, 2016, s.68; Hepaksaz ve Hayrullahoğlu, 2011, s.119). Elektronik devlet uygulamalarının ortaya çıkışı, gelişimi ve etkin bir şekilde kullanımının, kamu kurumlarının vatandaşlara ve paydaşlarına sunduğu hizmetlerin hızı, verimliği ve etkinliği üzerinde olumlu etkisi bulunmaktadır (Öz ve Bozdoğan, 2012, s.72).

Kurumlar ve paydaşları arasında var olan iletişimin en temel öğelerinden biri bilgi ve belge paylaşımıdır. Kurumlar bilgi ve belge paylaşımını gerçekleştirmek amacıyla birden fazla yöntem kullanmaktadır. Belge paylaşımının ilk örnek kullanım şekli yüz yüze yani fiziksel olarak gerçekleşmekte iken zaman içerisinde posta yöntemi kullanılmaya başlanmıştır. Posta yolu ile belge iletiminde postanın iletilip iletilmediğinden emin olmak amacıyla, iadeli taahhütlü olarak gönderim yöntemi geliştirilmiş ve kullanılmaya başlanmıştır. İlerleyen yıllarda teknolojinin faks ve elektronik posta (e-posta) imkânlarını sağlaması sonucunda bilgi ve belge gönderiminde yeni iletişim kanalı oluşmuştur ve bu yeni iletişim kanalı giderek artan bir şekilde kullanılmaya başlanmıştır. Bilgi ve belge iletişiminde güvenliğin sağlanması için en temel kontrol öğeleri, bilgi ve belgenin kim tarafından ne zaman, nerede ve hangi yöntemle paylaşıldığının kayıt altına alınmasıdır. Temel kontrol öğelerinin güvenli olarak sağlanması sonrası belgenin güven içerisinde olduğundan ve değiştirilmediğinden emin olarak saklanması gerekmektedir. Bilgi ve belgenin değiştirilmemesi ve uzun süre kayıt altında olması yönetimsel sürecin önemli ihtiyaçlarından biridir (Güler ve Furat, 2022, s.80).

E-postanın ortaya çıkışına bakıldığında: İnternet teknolojisinin temelleri 1969 yıllarına dayanmaktadır (Paloque-Bergès ve Schafer, 2019, s.3). İnternet teknolojisinin temel çalışma yöntemi verilerin paketler halinde bir noktadan başka bir noktaya çeşitli yollar takip ederek ulaşmasıdır. Veri paketleri, hedef noktaya ulaştığında birbiri ile ilişkili olanlar tek bir bütün olacak şekilde birleştirilmek suretiyle veri aktarımı tamamlanmış olur. Ray Tomlinson tarafından 1971 yılında internet üzerinde çalışan e-posta yazılımı geliştirilmiştir (O'Regan, 2018, s.124). Zaman içerisinde yapılan geliştirmeler sayesinde günümüzdeki kullanım haline bürünmüştür.

Bir e-posta, temel olarak başlık ve gövde olmak üzere iki bölümden oluşmaktadır. E-

postanın başlık bölümü 7-bitlik ASCII kodlamasına sahiptir. Bu başlık bölümünde konu, alıcı, gönderen, e-posta kimlik kodu ve yanıtlama adresi bulunmaktadır. Bir e-postanın yaşam döngüsü ele alındığında, göndericiden alıcıya kadarki süreçte işleme tabi tutulduğu sunucular üzerinde yönlendirme bilgileri ilgili sunucu tarafından başlığa eklenmektedir. Yönlendirme bilgileri kendi içinde zaman damgasına sahiptir. Zaman damgası bilgisi aracılığıyla bir e-postanın göndericiden alıcıya kadarki sürecinin ne kadar zaman aldığı bilinmektedir. (Varol ve Baştürk, 2014, s.273)

E-posta, internetin yaygınlaşması ile beraber iletişim aracı olarak etkin bir şekilde kullanılmaya başlanmıştır. İletişim yönüyle değerlendirildiğinde etkin, hızlı ve düşük maliyetli bilgi ve belge aktarımı sağlaması, yaygınlaşmasında önemli bir etkendir. Zaman içerisinde belgenin tarafları, özellikle kamu kurumları bilgi ve belge gönderiminde elektronik posta kullanımını artırmıştır.

E-posta her ne kadar iletişimde etkin bir biçimde kullanılıyor olsa dahi teknik açıdan değerlendirildiğinde güvenlik problemleri bulunmaktadır. Bu nedenle yetkili merciler tarafından değerlendirmeye alınırken yasal yönüyle kanıt olarak kullanılmasından kaynaklanan problemler bulunmaktadır. E-posta güvenliğinde problemlerden biri başlığa eklenen bilgilerdir. Kötü amaçlar için oluşturulmuş sunucular tarafından e-posta başlık bilgileri değişikliğe uğratılabilmektedir. (Foster vd. 2015, s.451). E-posta'da bulunan bu güvenlik problemlerinden ve bilgi belge yönetiminin daha verimli olması ihtiyacından dolayı kamu kurumları alternatif çözümler geliştirme yoluna gitmiştir (Amoroso, 2018).

Kamu kurumları kendi içinde bilgi ve belge yönetimini elektronik belge yönetim sistemi (EBYS) ile çözmektedir. Türkiye'de EBYS ile ilgili çalışmalar 2000'li yıllarda ortaya çıkmıştır. Hukuki altyapısı 2004 yılında 5070 sayılı kanunun yürürlüğe girmesinin ardından EBYS referans kriterlerinin 2005 yılında yayınlanması ile gerçekleşmiştir (Yalçınkaya, 2015, s.22; Kandur, 2011, s.6). EBYS'de bilgi ve belge güvenliği, bilginin bütünlüğü denetimi, belge üzerinde herhangi bir değişiklik yapılıp yapılmadığı güvence altına alınmaktadır (TSE, 2014, s.26).

Bu çalışmada değerlendirmeye alınan problem, bilgi ve belgenin kamu kurumundan muhatabına iletilmesi sürecinde güvenliğin ve doğruluğunun sağlanmasıdır. Bu nedenle kurumlar, kurum dışına iletilmiş olan belgelerin kendilerine ait olan EBYS aracılığı ile doğrulanması yolunu kullanmaktadır. Belgenin doğrulanması, iletişim açısından ihtiyaçları kısmi olarak karşılamaktadır. Temel problem kamu kurumunun bilgi ve belgenin tamamen ve reddedilemez şekilde muhatabına iletilmesi ve tebliğ işleminin gerçekleştirilmesidir. Bu amaçla tebliğ edilecek belgeler iadeli taahhütlü posta yönetemi kullanılarak gönderilmiştir ve teknolojinin sağladığı imkânların kullanılması ile muhatabın beyan ettiği e-postaya gönderim yöntemi yaygın olarak kullanılmıştır (Shermis ve Lombard, 1999, s.352; Öztürk, 2019, s.52). E-postanın eksik kaldığı yönlerinin telafi edilmesi amacıyla, temel çalışma prensibi benzer olan EBYS ve benzeri yazılımlar alternatif olarak kullanılmıştır. Alternatif çözümler arasında en çok tercih edilen yöntemlerden biri Kayıtlı Elektronik Posta (KEP) sistemidir.

Günümüzde kamu kurumlarının, kurum dışına belge bilgi gönderimi gerçekleştirirken tercih ettiği en yaygın uygulama KEP sistemidir. Çalışmanın devamında KEP sistemi kavramsal ve uygulama olarak incelenmiş olup, dünyada var olan ilk uygulama örnekleri hakkında bilgi verilmiştir. Ardından Türkiye Cumhuriyeti'nde kullanımı ve kullanımı

teşvik edici yasal altyapısı ilgili düzenlemeler hakkında bilgiler verilmiştir. KEP sisteminin teknik yönleri açıklanmıştır. KEP sisteminin kullanılması durumunda kurumsal boyutta sağladığı faydalar açıklanmıştır.
KEP sistemi hakkında bilgiler verilmesi sonrası blok zincir teknolojisine ait kavramsal çerçeveyi oluşturan bilgiler verilmiştir. KEP sisteminin, uygulama yönteminden dolayı gerçekleşmesi olası güvenlik problemleri açıklanmış ve blok zincir teknolojisinin kullanımı ile söz konusu olası güvenlik problemlerine yönelik çözüm öneri olarak sunulmuştur. KEP sisteminde blok zincir teknolojisi kullanımı ile güvenlik problemlerine sunulan çözüm önerisi çalışmanın özgün yönünü oluşturmaktadır.

KEP Tanımı

Kayıtlı Elektronik Posta sistemi, e-posta ile gerçekleştirilen haberleşme yönteminin düzenleyici kurumlar tarafından yetkilendirilmiş hizmet sağlayıcılar vasıtasıyla bilgi ve belge aktarımını sağlayan sistem olarak tanımlanabilir. KEP sistemi, temel çalışma prensibi olarak e-posta gibi olsa dahi kendi içinde alınan güvenlik önlemleri açısından e-postadan çok ayrı bir noktada değerlendirilmelidir. KEP sistemi, elektronik imza ve zaman damgası ile sistem içerisinde yürütülen süreçlerde iletinin erişiminin garanti altına alınması, iletinin taraflarının kimliklerinin reddedilemez şekilde kayıt edilmesi ve doğrulanması diğer bir taraftan süreç içerisinde iletinin değişikliğe uğramadığından emin olunmasını sağlamaktadır. KEP sistemi içerisinde ileti aktarımı süreci içerisinde, güvenlik amaçlı geliştirilen önlemlerin oluşturduğu kayıtlar yasal merciler tarafından kabul edilebilir kanıt niteliğindedir (Bayram ve Karabalık, 2015).

KEP sistemi uluslararası alanda Registered E-mail (REM) olarak bilinmektedir. KEP sisteminin ilk örnekleri, 2004 yılında DDS Avusturya, 2005 yılında PEC İtalya, 2009 yılında De-Mail Almanya, 2010 yılında Moja.posta.si adıyla Slovenya'da ortaya çıkmıştır. Devam eden yıllarda KEP sisteminin yaygınlaşması ve diğer ülkelerde kabul görmesi üzerine özel posta operatörleri tarafından 2010 yılında Almanya'da E-postbrief, 2011 yılında İsviçre'de IncaMail ve İspanya'da Apartado Postal ve Kanada'da PosteCS kurulmuştur. Özel sektör tarafından 2011 yılında Belçika'da CertiPost ve ABD'de Rpost hayata geçirilmiştir. Tüm Avrupa Birliğini kapsayan ancak halen proje aşamasında olan Pan-european Public Procurement Online (PEPPOL) çalışmaları devam etmektedir (Yılmaz ve Üstündağ, 2015, s.211; Ruggieri, 2010, s.314; Berber, 2009, s.197; Bayram ve Karabalık, 2015, Tauber, 2011).

KEP sistemi Türkiye Cumhuriyeti'nde de kullanılmaktadır. Türkiye'de KEP sisteminin düzenleyicisi Bilgi Teknolojileri ve İletişim kurumudur (BTK). BTK, KEP hizmet sağlayıcıların yeterli bilgi güvenliğine sahip olup olmadığının kontrolü ve yetki verme konusunda yetkili mercidir (Samast, 2017; Bayram ve Karabalık, 2015). BTK hizmet sağlayıcıların yetkilendirilmesini ve denetimini Avrupa Telekomünikasyon Standartları Enstitüsü'nün (ETSI) ilgili konudaki düzenlemelerine uygun olarak gerçekleştirmektedir. Hali hazırda BTK tarafından yetkili hizmet sağlayıcısı olarak tanınan 8 işletme bulunmaktadır. Bu işletmeler ile ilgili detaylar Tablo 1'de verilmiştir.

Tablo 1. KEP Hizmet Sağlayıcı Listesi (BTK, 2017)

İşletme Adı	Faaliyete Başlama Tarihi	Alan Adı	Web Sitesi

Posta ve Telgraf Teşkilatı A.Ş.	10.09.2012	hs01.kep.tr	http://www.ptt.gov.tr
TNB Bilişim Teknolojileri Sanayi ve Ticaret Anonim Şirketi	28.12.2012	hs02.kep.tr	http://www.tnbkep.com.tr/
TÜRKKEP Kayıtlı Elektronik Posta Hizmet Sağlayıcılığı ve Ticaret A.Ş.	25.02.2013	hs03.kep.tr	http://www.turkkep.com.tr/
INTERTECH Bilgi İşlem ve Pazarlama Ticaret A.Ş	14.11.2014	hs04.kep.tr	https://www.inter-kep.com.tr
EFINANS Elektronik Ticaret Ve Bilişim Hizmetleri A.Ş.	05.02.2015	hs05.kep.tr	http://www.efinans.com.tr/tr/urun-ve-hizmetler/KEP
KEPKUR Yazılım Bilişim Kayıtlı Elektronik Posta Hizmetleri Sanayi Ve Ticaret A. Ş.	11.09.2015	hs06.kep.tr	https://www.kepkur.com.tr
F.I.T. Bilgi İşlem Sistemleri Servisleri Sanayi ye Ticaret A.Ş.	11.09.2015	hs07.kep.tr	http://www.fitsolutions.com.tr
Mikro Yazılımevi Yazılım Hizmetleri Bilgisayar Sanayi ve Ticaret A.Ş.	14.01.2016	hs08.kep.tr	http://www.mikrokep.com.tr

Türkiye'de KEP Mevzuatı

Türkiye'de KEP ile ilgili ilk atıf 2011 tarihli 6102 sayılı Türk Ticaret Kanunu'nda gerçekleştirilmiştir. İlgili düzenlemede tüccarlar arasındaki temerrüde düşürme, sözleşme feshi ve benzeri ihbar veya ihtarların KEP ile yapılacağı belirtilmiştir. Aynı düzenleme, KEP sistemi için ikincil düzenleme yapma yetkisini BTK'ya vermiştir (Resmi Gazete, 2011; Varol ve Baştürk, 2014, s.272). Türkiye'de KEP ile ilgili yapılan düzenlemeler aşağıdaki gibidir (Yılmaz ve Üstündağ, 2015, s.212; Öztürk, 2019, s.38; BTK, 2017):

- Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 25.08.2011 tarih ve 28036 sayılı Resmi Gazete

- Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 25.08.2011 tarih ve 28036 sayılı Resmi Gazete
- Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, 16.05.2012 tarih ve 28294 sayılı Resmi Gazete
- Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul Esaslar, 06.06.2012 tarih ve 2012DK-15259 sayılı Kurul Kararı
- Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar yayımlanmasına ilişkin Kurul Kararı, 09.09.2014 tarih ve 2014/DK-BTD/447 sayılı Kurul Kararı
- Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar

Literatür Özeti

Bayram ve Karabalık yaptıkları çalışmada, e-tebligat ve KEP uygulamalarını ele almış ve kurumların KEP'e geçiş için gerekli olan yasal alt yapıyı ve aşamalarını açıklamıştır (Bayram ve Karabalık, 2015, s.148). Varol ve Baştürk, KEP uygulamasını hukuki alt yapısı yönüyle incelenmiş ve teknik boyutuyla detaylandırmıştır (Varol ve Baştürk, 2014). Üstündağ ve Yılmaz yaptıkları çalışmada, kamu kurumlarının KEP sistemine etkin ve verimli geçişinin sağlanması için gerçekleştirilmesi ve gözden geçirilmesi gereken süreçleri değerlendirmiş ve öneriler sunmuşlardır (Yılmaz ve Üstündağ, 2015). Öztürk, yüksek lisans tezinin bir bölümünde, Türkiye'de e-devlet süreci içerisinde KEP uygulamasını ve dünyadaki örneklerini incelemiştir (Öztürk, 2019, s.31). Eker, kayıtlı elektronik posta sistemini hukuki boyutları ele almış ve KEP sisteminin e-postanın güvenli hali olduğunu ve e-tebligat'ın ise KEP sisteminin bir alt kullanım şekli olduğunu belirtmiştir (Eker Kitiz, 2019, s.16). Emam, yaptığı çalışmada KEP sisteminin bulut bilişim alanında kullanımının artış göstereceğini ön görmüş ve bulutta kullanımı durumunda arttırılmış yetki ve yetkilendirme metodu önerisinde bulunmuştur (Emam, 2013, s.112). Türkçe kaynaklarda yapılan çalışmalara bakıldığında KEP sisteminin sadece yasal altyapısı incelenmiş olup kurumlara verimlilik açısından etkileri değerlendirilmiştir. Teknik açıdan eleştirel ve alternatif metot önerisi olmadığı tespit edilmiştir.

Hinarejos ve ark. tarafından Bitcoin tabanlı protokol tasarlanmıştır. Ancak yaptıkları çalışmanın eksikliği bulunmaktadır. Yapılan çalışmada, alıcıya iletilen mesajı şifreleyen anahtarı doğrulama imkanı bulunmamaktadır. Bu nedenle gönderen taraf mesajı gönderebilir ancak teslim alan taraf mesajı okuyamama durumunda kalabilir. Hinarejos ve Ferrer-Gomila çok taraflı sertifikalı mesaj gönderimine yönelik yeni protokol önermişlerdir ancak doğrulama anahtarı ile ilgili problem devam etmektedir (Hinarejos ve ark., 2019; Hinarejos ve Ferrer-Gomila, 2020).

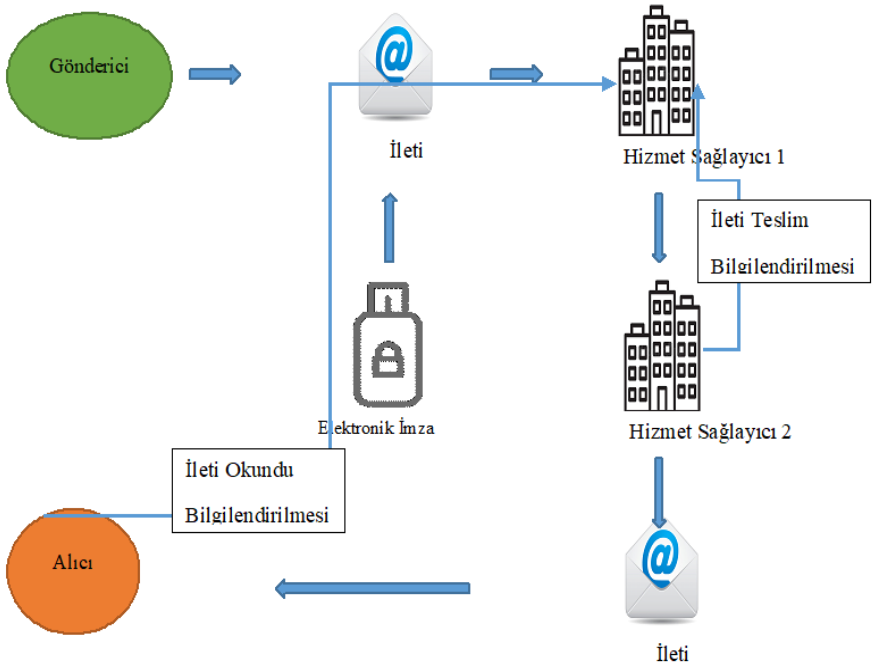
Mut-Puigserver ve ark. akıllı sözleşme kullanarak sertifikalı mesaj gönderimi konusunda çalışma yürütmüştür. Bu alanda toplam olarak 4 adet yayın yapmışlardır. Yaptıkları çalışmalarda iki adet protokol geliştirmiş olup ilk protokolde mesaj gönderimi üçüncü tarafa güven gerektirmediği durumda mesaj içeriğinin erişilebilir olarak belirlemişlerdir. Ancak üçüncü tarafın güvenliği protokole eklediklerinde mesaj içeriğini gizlemişlerdir. Son yaptıkları çalışmada üçüncü tarafa güven gerektirmeden ve mesaj gizliliği sağlanarak protokolü güncellemişlerdir. Ancak bu yeni protokolde yapılan işlemlerin maliyetleri yüksek olması nedeniyle uygulanabilirliği konusunda şüphe duyulmaktadır

(Mut-Puigserver, Payeras-Capellà ve Cabot-Nadal, 2018; Mut-Puigserver, Payeras-Capellà ve Cabot-Nadal, 2018b; Payeras-Capella, Mut-Puigserver ve Cabot-Nadal, 2019; Mut-Puigserver, Cabot-Nadal ve Payeras-Capellà, 2020). Bu çalışmada, üçüncü bir tarafa ihtiyaç duyulmadan, mesaj gizliğini iki taraf arasında gerçekleştirilen anahtar aracılığı ile sağlayan ve akıllı sözleşmeye dayalı ve daha önceki çalışmalara göre daha düşük maliyetli bir çözüm ortaya koyulmuştur.

KEP Sisteminin Çalışma Şekli

KEP ile ilgili mevzuat kapsamında ve KEP hizmet sağlayıcıların web sitelerinden elde edilen çalışma yöntemine Şekil 1'de yer verilmiştir (PTT, 2022; BTK, 2017; Mikrokep, 2022; Tosun, 2016).

Şekil 1. KEP Sisteminin İşleyişi (Yazar tarafından çizilmiştir)



Şekil 1'de verilen süreç özetle aşağıdaki gibidir:

- Gönderici iletisini oluşturur ve elektronik imza ile imzalar.
- Oluşturulan ve imzalanan ileti hizmet sağlayıcısına gönderilir.
- Hizmet sağlayıcı 1 adres bilgisine uygun olarak bir başka hizmet sağlayıcı 2'ye gönderir.
- İleti hizmet sağlayıcı 2'ye ulaştığında iletinin teslim alındığına dair imzalı ve zaman damgalı bilgi iletilir.
- Alıcı tarafından ileti açıldığında iletinin okundu bilgisi imzalı ve zaman damgalı olarak servis sağlayıcısı 1'e iletilir.

KEP Sisteminin Faydaları

Kurumlar açısından KEP kullanımının yazışmalarda hız kazanmanın yanında maliyet ve güvenlik faydası bulunmaktadır. KEP sisteminin genel olarak aşağıdaki gibidir (Yılmaz ve Üstündağ, 2015, s.214):

- İletinin gönderici kimlik bilgisinin reddedilemeyecek şekilde kayıt altına alınması
- İletinin üretilme zaman bilgisinin reddedilemeyecek şekilde kayıt altına alınması
- İletinin alıcı tarafına ulaşıp ulaşmadığı bilgisinin reddedilemeyecek şekilde kayıt altına alınması
- İletinin alıcı tarafından okunup okunmadığı bilgisinin reddedilemeyecek şekilde kayıt altına alınması
- Gönderici ve alıcı tarafında sürecin hızlı olarak gerçekleşmesi vasıtasıyla zamandan tasarruf
- Gönderici ve alıcı arasında belge aktarımının maliyetinin azaltılması
- Gönderici ve alıcı arasında oluşan veri trafiğinin tümünün kayıt altına alınması ve en az 20 yıl boyunca saklanması.
- Gönderi ve alıcı tarafında iletişimin zaman ve mekândan bağımsız olarak gerçekleştirilmesi

KEP sistemi teknik yönüyle faydalı olmasının yanında iletilerin fiziki imkânlar ile gönderilmesinden kaynaklı zaman kaybını engellemektedir. KEP sistemi, kimi zaman belgelerin muhatabına ulaşmaması, iletilecek adresin bulunamaması gibi nedenlerden dolayı ortaya çıkan problemleri ortadan kaldırmaya aday bir yöntem olarak değerlendirilmektedir (Yurtsever, 2016, s.463).

Elektronik imkânların henüz kullanılmadığı zamanlarda kurumlar muhataplarına bilgi ve belge aktarımlarını posta yolu, memur eliyle, ilanen ve kapıya yapıştırma yöntemi ile sağlamıştır. Bilgi belge aktarımında en fazla problem yaşanan belge türü tebligattır. Tebligat ile muhatap olmamak için bireyler yanlış adres bilgisi verebilmektedir. Kimi zaman usul olarak tebligat süreçlerinde de hata yapılmaktadır. Bu hatalar nedeniyle iletilen belgeler geçersiz olarak değerlendirilmekte ve tekrar usul ve esaslar çerçevesinde yollanması gerekmektedir. Posta yoluyla belge aktarımında muhatabın bilinen son adresine belge iletilir veyahut memur eliyle teslim edilir. Belge teslim edildiğinde teslim tarihi tebliğ tarihi olarak kabul edilmektedir. Kimi zaman posta ve memur eliyle ilgili tarafa ulaşılamamaktadır. Bu durumda ilanen tebliğ yöntemi kullanılmaktadır. İlanen tebliğ yönteminde, bilgi ve belgelerin yayın araçları kullanılarak veya duyuru panoları gibi alanlara asılması suretiyle muhataba ulaşılmaya çalışılmaktadır. Bilgi ve belge aktarma yöntemlerinden de anlaşılacağı üzere elektronik yöntemlerin etkin bir şekilde kullanılması zaman açısından verimliliği sağlamaktadır (Beceriklican, 2019, s.17; Arslan ve Biniş, 2016).

KEP sistemi, elektronik iletişimin bir yönetimi olarak kabul edilmektedir. Bu nedenle elektronik olmayan iletişim kanalları ile karşılaştırıldığında birim maliyetleri düşük bir yöntemdir. Belge iletiminin yoğun olduğu kurumlarda maliyetlerin düşeceği öngörülmektedir. Bu açıdan değerlendirildiğinde olumlu ekonomik etkisi

bulunmaktadır (Börü, 2012, s.405).

Klasik yöntemler ile belgelerin iletimi gerçekleştirildiğinde kâğıt kullanılmaktadır. Kâğıt kullanımı gerektiren yöntemlerin çevreye olan olumsuz etkisi kaçınılmaz bir gerçektir. Kâğıt üretimi sürecinde gerek doğadan eksiltilen ağaçlar problem iken diğer taraftan kâğıt üretimi ve belgenin fiziksel olarak hazırlanması ve iletiminde ortaya çıkan karbon ayak izinin büyüklüğü çevreye ciddi zarar vermektedir. Fiziksel bir belge sadece kâğıttan ibaret değildir. Fiziksel belge, üretilirken harcanan enerji ve işgücü, basımı sırasında kullanılan yazıcı ve toner masrafı, iletimi sırasında kullanılan işgücü, postalama masrafları ve fosil kaynaklı tüketilen yakıt demektir (Bayram ve Karabalık, 2015, s.152).

Blok Zincir Teknolojisi

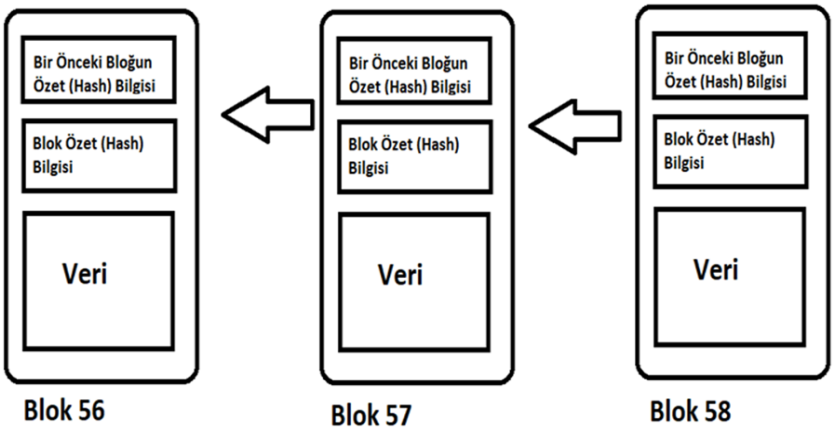
Blok zincir teknolojisi 2008 yılında Nakamoto tarafından yazılan makale ile ortaya konulmuştur. Makalede verilerin bloklar halinde saklanması ve blokların içinde bulunan verinin özet bilgisinin bir sonraki bloğa eklenmesi suretiyle güvenliğinin ve değişmezliğinin sağlanması amaçlanmıştır (Şekil 2). Kayıt altına alınan veriler birden fazla noktada birer kopyası saklanmaktadır (Brito ve Castillo, 2013; Nakamoto, 2008).
Blok zincir teknolojisinin temel taşını oluşturan teknolojiler, özetleme, açık anahtar şifreleme yöntemleri, sayısal imzalama, eşler arası ağlar ve mutabakat yöntemleridir. Blok zincir teknolojisi asimetrik şifreleme yöntemi kullanmaktadır. Asimetrik şifreleme yönteminde 2 adet anahtar bulunmaktadır. Açık anahtar ile güvenli olarak mesaj iletiminin kontrolü ve kimlik doğrulama işlemleri gerçekleştirilmektedir. Kapalı şifreleme ile kayıt altına alınan verilerin gizlenmesi ve sadece kapalı anahtara sahip tarafların verileri okuyabilmesi sağlanmaktadır (Rivest, 1978; Aydar, 2019). Eşler arası ağlarda, genellikle kullanılan istemci-sunucu mimarisinden farklı bir işleyiş bulunmaktadır. İstemci-sunucu mimarisinde veri kaynağı merkezi bir sunucudur. Bu nedenle en üst yetkili seviye olarak sunucu görülmekte ve ağ içerisinde geri kalan iletişim noktaları istemci olarak daha az yetkili olmaktadır. Eşler arası ağlarda, ağ üzerinde faaliyet gösteren tüm düğüm noktaları eşit olarak kabul edilmektedir. Ağ üzerinde bulunan düğümler merkezi bir sunucuya ihtiyaç duymadan iletişim kurmakta ve faaliyet göstermektedir. Eşler arası paylaşılan verilerin nihai olarak kayıt altına alınması mutabakat protokolü ile sağlanmaktadır. Blok zincir teknolojisinde mutabakat protokolü olarak birden fazla yöntem bulunmaktadır. Ancak en yaygın olan mutabakat protokolleri İş kanıtı (Proof of Work - PoW) ve Hisse kanıtı (Proof of Stake - PoS) metotlarıdır (CNIL, 2018, Xue ve diğerleri, 2018, s.637).

İş kanıtı mutabakat protokolünde, bilgi bloğu yayınlanmadan önce kendisinden önce oluşturulmuş blokların özet bilgisi temel alınarak bir problem oluşturulur. Bu problemi ilk çözen düğüm veri bloğunu blok zincir ağı üzerinde yayınlamaya yetkili olur (Nakamato, 2008). Hisse kanıtı mutabakat yönteminde, düğümlerin sahip oldukları varlıkları onaylama sürecine katılmak amacıyla kilitlemesi ile gerçekleşmektedir. Blok zincir ağında kilitli olan varlık miktarının oranına göre onaylama sürecine dâhil olunmaktadır (Conoscenti, Vetro ve De Martin, 2016). İş kanıtı yönteminde, blok onaylama sürecinde işlem gücüne ihtiyaç duyulmaktadır. Blok zincirin kontrolünün sağlanması için tüm ağda bulunan işlem gücünün %51'i kadarının kontrol altına alınması gerekmektedir. Hisse kanıtı yönteminde, blok onaylamak için varlıklar kilitlenmektedir. Hisse kanıtı mutabakat yönteminin kullanıldığı bir blok zincir ağında ağ kontrolünün sağlanabilmesi için ağ üzerinde kilitli olarak saklanan varlıkların büyük bir kısmının elde tutulması gerekmektedir. Bu nedenle blok zincir ağının kontrolünün ele geçirilmesi

zordur ve iş kanıtı yöntemine göre kıyaslandığında da daha maliyetlidir (Yang, Chen, ve Chen, 2019; Ye, Li, Cai, Gu ve Fukuda, 2018; Gaži, Kiayias ve Russell, 2018; Hao, Li, Dong, Fang ve Chen, 2018).

Blok zincir ağı, veri saklama için kullanılmaktadır. İlk ortaya çıkan örneği Bitcoin ağıdır. Ancak zaman içerisinde ihtiyaçlardan dolayı farklı ağlar ortaya çıkmıştır. Ortaya çıkan ağlar veri gizliliği ve düğümlerin sınırlandırılması amacıyla farklı yapılarda oluşturulmuştur. Bu nedenle blok zincir ağları tür yönüyle açık, kapalı ve hibrit olmak üzere 3 temel yapıya sahiptir. Açık blok zincir ağları, zincir üzerinde verilerin herkes tarafından görülebildiği ve mutabakat sürecine izin gerektirmeden katılım sağlandığı yapıdır. Kapalı blok zincir ağı, blok zincir üzerinde verilerin kapalı olduğu ve mutabakat sürecine sadece izinli düğümlerin katılabildiği ağ türüdür. Hibrit blok zincir ağında ise veriler ve mutabakat sürecine katılım izni ayrı ayrı olarak düzenlenmekte ve blok zincir üzerinde izinler tamamıyla veya kısmi olarak verilmektedir (Liu ve Fraser, 2018; Khan, Zahid, Hussain, Farooq, Riaz ve Alam, 2019).

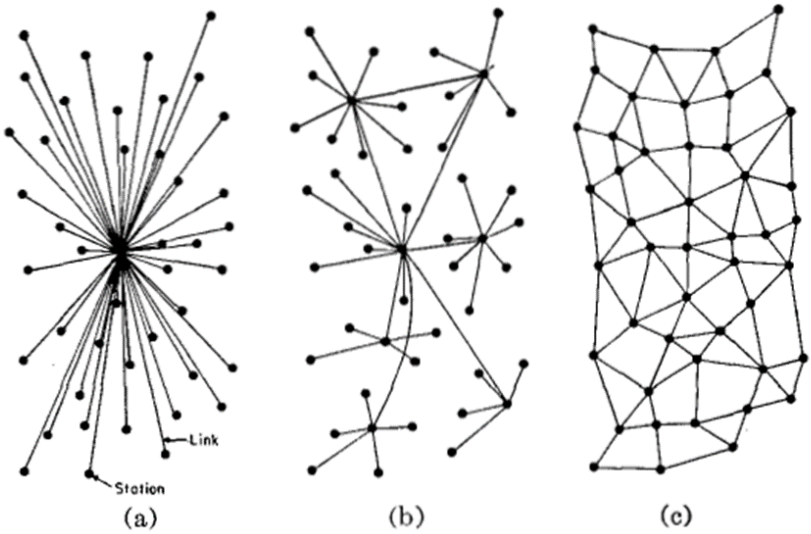
Blok zinciri teknolojisi sadece veriyi güvenli olarak saklamak ve veriye tekrar ulaşmak gibi sınırlı bir göreve sahiptir. Güvence altına alınan veri değiştirilememekte, dağıtık ve şeffaf bir şekilde saklanmaktadır. Blok zincirinin uygulamada ortaya çıkan ilk örnekleri basit varlık oluşturulması ve bu varlığın kayıt altına alınması şeklinde olmuştur. Ancak günlük hayatta var olan ihtiyaçlar bu görevlerden daha karmaşıktır. Gerçek hayat problemlerinde varlıkların ya da verinin önceden belirlenmiş olan kurallar çerçevesinde tepki vermesine ihtiyaç duyulmaktadır. Bu durumda blok zincir teknolojisinde verinin kurallara göre hareket etme ihtiyacı ortaya çıkmaktadır. Bir dizi kuralın tetiklenmesi ve bunun sonucunda verinin tek veya birden fazla taraf ile etkileşime girmesini sağlayan akıllı sözleşme teknolojisi blok zincir üzerine entegrasyonu gerçekleştirilmiştir. Akıllı sözleşmeler ilk olarak Ethereum projesi ile ortaya çıkmıştır. Akıllı sözleşmeler blok zincir ağı üzerinde saklanan kod betiklerinin ihtiyaç halinde çağrılması ile belirlenmiş görevlerin gerçekleştirilmesi teknolojisidir (Clack, Bakshi ve Braine, 2016; De La Rosa ve diğerleri, 2017). Akıllı sözleşme teknolojisinin ilk uygulandığı blok zincir ağında, akıllı sözleşmeler solidity adı verilen bir programlama dili ile kodlanmaktadır. Daha sonra ortaya çıkan farklı blok zincir ağlarında assemblyscript, go ve rust programlama dilleri ile de akıllı sözleşme kodlama imkânı bulunmaktadır. Akıllı sözleşmelerin kullanımı ile birçok alanda blok zincir teknolojisinin kullanımı giderek artmaktadır (Prasad, 2018). Blok zincir ve akıllı sözleşme veri, varlıkların kayıt altına alınması ve finansal süreçler ile ilgili sektörlerde etkisi büyüktür (Garfinkel ve Drane, 2016). Ancak zaman içerisinde blok zincir ve akıllı sözleşme teknolojisinin kabul edilmesi arttıkça kullanıldığı sektörler tarım, sağlık, sigortacılık, mülkiyet ve tedarik zinciri gibi sektörlere doğru yayılmıştır (Carson, Romanelli, Walsh ve Zhumaev, 2018; Nussbaum, 2017).



Şekil 2. Blok Zincir Yapısı (Nakamato, 2008, s.6)

Akıllı sözleşmeler, web teknolojilerinin etkileşimi ile merkezi olmayan uygulamaların ortaya çıkmasını sağlamıştır. Merkezi olmayan uygulamalar, temel olarak son kullanıcıların web veya mobil bir arayüzü kullanarak blok zincir ve akıllı sözleşmelere ile etkileşime girdiği uygulamalardır. Merkezi olmayan uygulamalar genellikle blok zincir ağı ile API aracılığı ile iletişime girmektedir. Merkezi olmayan uygulamalar, merkezi bir işlem ve depolama birimine ihtiyaç duymadan çalışabilen yazılımlardır. Merkezi olmayan uygulamalarda (Şekil 3), verileri genellikle blok zincir üzerinde saklanmaktadır ancak veri kayıt imkanı sınırlıdır. Bu nedenle daha büyük veri saklama ihtiyacı IPFS gibi merkezi olmayan merkezi olmayan depolama alanlarında saklanmaktadır (Allison, 2016; Jamil ve diğerleri, 2019; Sharma, 2018).

Merkezi olmayan teknolojik çözümler blok zincir teknolojisinin gerçek hayat problemlerini çözmesinde son kullanıcı tarafının oluşturulmasında nihai arayüzüdür. Merkezi olmayan çözümler geliştirilmesi durumunda üç temel katmanın bir biriyle iletişime geçmesi ile gerçekleşmektedir. Merkezi olmayan uygulamalarda ilk katman, blok zincir katmanıdır. Bu katman blok zincir temelinde oluşturulmuş çözümler için zincir yapısını sağlamaktadır. İkinci katman, blok zincir ile iletişim için gerekli ara katmandır. Yazılım geliştirme ve ölçeklendirme süreçlerini kolaylaştırmaktadır. Son katman ise merkezi olmayan uygulamalar katmanıdır. Son kullanıcının bir web veya mobil uygulama ile blok zincir ile iletişimin sağlayan katmandır. Bu katmanda genellikle iletişim API'ler üzerinden sağlanmaktadır. Merkezi olmayan uygulamalar çoğunlukla bu katmanda gerçekleştirilmektedir (Karaarslan ve Birim, 2021).



Şekil 3. Merkeziyet Yapısına Göre Uygulamalar (a) Merkezi, (b) Merkezi olmayan, (c) Dağıtık (Buterin, 2017)

Problemin tanımı ve çözüm önerisi

KEP sistemi güvenlik ve kontrol açısından birçok avantajı bulunmaktadır. Kendi içinde belirlenmiş güvenlik standartlarına göre veri güvence altına alınmaktadır. Verinin bir noktadan başka bir noktaya iletilmesi sonucunda kaynağın kontrolü iletilen veri paketinin dijital ve zaman damgası ile gerçekleştirilmektedir. KEP sistemi içerisinde işlem yapacak olan tarafın daha önceden sistem tarafından kimlik kaydı yapılmış olup giriş için kendisine verilmiş olan kimlik ile giriş yapmakta ardından veri ekleme işlemi için dijital imza kullanarak kimliğini tekrar kanıtlamaktadır ve ardından veri kayıt altına alınmaktadır. Ancak kayıt altına alınan veri, veriyi ekleyen tarafın hizmet aldığı servis sağlayıcının sistemleri üzerinde kayıt altına alınmaktadır. Eğer eklenen verinin iletilmesi gereken alıcı taraf başka bir hizmet sağlayıcı firmada ise verinin bir kopyası da alıcı tarafın hizmet sağlayıcısında saklanmaya başlar.

KEP sistemi, yazılım mimarisi açısından değerlendirildiğinde merkezi yazılım mimarisine sahiptir. Merkezi yazılım mimarisinde işlemler tek bir merkezde gerçekleştirilir ve veri yedekleme ve ölçeklendirme ihtiyaçları haricinde tek bir noktada saklanmaktadır. Bu yapı doğası gereği aşağıda belirtilen özelliklere sahiptir:

- Hizmet sağlayıcıya güven: Hizmet sağlayıcı firmanın kendisine emanet edilen verileri saklamakla yükümlüdür. Hizmet sağlayıcı firmanın veriyi saklama yöntemine ve veriyi değiştirmediğine güven üzerine kuruludur. Hizmet sağlayıcının verileri uluslararası standartlarda sakladığı kabul edilmektedir. Hizmet sağlayıcının gerçekleştirdiği veri operasyonları halka açık olmamasından dolayı kontrolü gerçekleştirilmesi sınırlıdır.

- Zaman sunucusuna güven: Hizmet sağlayıcı için verilerin kendisi tarafından değiştirilmediğinin ya da başkaları tarafından değiştirilmediğinin en temel güvencelerinden biri zaman damgasıdır. Hizmet sağlayıcı zaman damgası kullanmak

için kendi içinde veya üçüncü bir taraftan zaman damgası hizmeti alabilmektedir. Hizmet sağlayıcının belirlenmiş zaman sunucusundan doğru zaman bilgisi aldığı kabul edilir. Ancak zaman damgası ile ilgili kesin güvenliğin sağlanması için üçün bir taraftan zaman damgası bilgisinin gelmesi gerekmektedir.

- Yasal mercilerin kontrolü: Hizmet sağlayıcıların belirlenmiş standartlarda hizmet verdiğinin kontrolü yasal mercilere bağlıdır. Ancak yasal mercilerin veya bu konuda yetkilendirilmiş kurum ve kuruluşların denetimi kurumsal kapasiteleri ile sınırlıdır. Bu nedenle hizmet sağlayıcı firmanın veri güvenliği ile ilgili güven sınırları, yasal mercilerin yaptırımları ve denetleme yetenekleri ile sınırlıdır.

- Siber güvenlik kapasitesi: Bilişim teknolojileri alanında siber güvenlik önemli bir konudur. Günümüzde gittikçe firmalar bilişim yönünden istismar edilmeye çalışılmaktadır. Bir bilişim altyapısının istismar edilmesi ve fark edilmesi arasında geçen süre ortalama 56 gündür (Rebovich ve Byrne, 2022). Bu nedenle hizmet sağlayıcının siber güvenlik kapasitesi önemlidir. Hizmet sağlayıcının bilişim altyapısında gerçekleşecek bir istismar verinin bütünlüğü ve doğrulanmasını ortadan kaldırır.

- Verilerin tek merkezde saklanması: Veriler merkezi bilişim sistemlerinde genelde tek merkezde saklanmaktadır. Verilerin yedeklerinin birden fazla noktada bulunması verilerin tek merkezde saklandığı gerçeğini değiştirmez. Yedekleme sistemleri sadece belirlenen zaman aralıklarında doğru kabul edilen verilerin bir kopyasını içermektedir. Siber güvenlik açısından bilişim altyapılarının ortalama olarak istismar edildikleri fark ettikleri süre dikkate alındığında yedeklerin istismardan kaçamayacaktır. Bu nedenle doğruluğu önemli hassas verilerin saklanmasında tek merkez uygulaması kendi içinde problemlere sahiptir.

Yazılımlar, merkezi mimariye alternatif olarak merkezi olmayan ve dağıtık yazılım mimarisi ile geliştirilme imkânına sahiptir. Merkezi olmayan veya dağıtık yazılım mimarisinde işlemler ve verilerin birden fazla merkezde kopyası saklanacak şekilde barındırmaktadır. Verilerin saklandığı her bir nokta düğüm olarak ifade edilmektedir. Düğümler kendi aralarında belirlenmiş protokoller ile haberleşmektedir. Merkezi olmayan veya dağıtık sistemler genellikle blok zincir teknolojisi ile beraber kullanılmaktadır. Blok zincir ve merkezi olmayan mimari benimsendiğinde aşağıda belirtilen avantajlara sahip olunmaktadır:

- Veri Kontrolü: Blok zincir teknolojisi kullanıldığında, zincir üzerine her yeni blok eklendiğinde daha önceden eklenmiş olan bloklar düğümler tarafından kontrol edilmektedir. Eklenecek zincir üzerinde herhangi bir veri istismarı tespit edilmemiş olması durumunda blok eklenmektedir.

- Verinin birden fazla kopyasının bulunması: Blok zincir üzerinde eklenen veri blokları birden fazla noktada saklanmaktadır. Veri bloklarının bir biri ile uyumlu olup olmadığı her blok üretiminde kontrol edilmektedir. Böylelikle blok zincire eklenen veri tek merkezde değil birden fazla merkezde saklanmaktadır.

- Zaman Damgası: Blok zincir ağında bulunan düğümler ağın zaman bilgisini kendi üzerinde saklamaktadır. Blok zincir ağında bulunan düğümler kendilerine komşu düğümler ile zaman bilgisini paylaşmaktadır. Zaman damgası için gerekli zaman bilgisi, blok zincir ağında bulunan komşu düğüm noktalarından gelen zaman bilgisinin medyanından oluşmaktadır. Düğüm kendisinde bulunan zaman değeri ile

komşularından elde ettiği zaman bilgisinin medya değeri arasında 70 dakikadan fazla bir fark elde etmesi durumunda zaman bilgisinin güvenli aralıkta olmadığını kabul etmektedir. Zaman bilgisine ait değer güvenli zaman aralığına sahip olmayan düğüm noktaları hesaplamaya dahil edilmez (Conti ve diğ., 2018, s.3424; Hasanova ve dig., 2019, s.31; Boverman, 2015).

- Mutabakat: Blok zincir teknolojisinde, her ağın blokların zincir üzerine eklenmesi için kendi içinde mutabakat protokolü bulunmaktadır. Blok zincir teknolojisinde en yaygın kullanılan mutabakat protokolü PoW ve PoS'tir. Mutabakat protokolü uyarınca bloğun zincir üzerine eklenmesi için onay alınması gereken minimum düğüm noktası sayısına ulaşması gerekmektedir. Blok zincir teknolojisinde kullanılan mutabakat protokolünün algoritmasına göre düğüm noktalarının yeterli sayıda doğrulamayı yapması beklenir, gerekli sayıya ulaşıldığında blok zincir üzerine eklenir ve ağ üzerinde zincirin kopyalarının saklandığı diğer düğümlerde kopyasının güncellenmesi sağlanır.

- Dağıtık sistem: Blok zincir teknolojisinin temel prensiplerinden biri tek merkeze güven olmadan verinin doğrulanması ve saklanmasıdır. Blok zincir teknolojisinde tek merkeze güven gerekli değildir. Bu amaçla veri bloğu oluşturulduğunda birden fazla düğüm üzerinde kontrol sağlanmakta ve düğüm noktaları sürekli olarak değişmektedir.

- Siber istismar zorluğu: Blok zincir teknolojisinde veri bloğunun zincir üzerine eklenebilmesi için düğümlerin mutabakat protokolüne göre onaylanması gerekmektedir. Mutabakat protokolü istismar edilmesi durumunda veri bloklarının bütünlüğü tehlikeye girmektedir. Teorik olarak mümkün olması ile birlikte fiili uygulamanın gerçekleşmesi kolay değildir. PoW mutabakat protokolü kullanan blok zincir ağında, zincir üzerinde faaliyet gösteren düğümlerin sahip olduğu işlem gücünün %51'i oranında hâkimiyet sağlanması gerekmektedir. Bu oranda işlemci gücünün sağlanabilmesi için gerekli maddi yatırım çok ciddi miktardadır ve blok zincir büyüdükçe gerekli işlemci gücü artmaktadır. PoS mutabakat protokolü kullanımında, varlık bulundurma ihtiyacı bulunmaktadır. Varlık büyüklüğü, düğümlerin varlık büyüklüğünün toplamının en az üçte biri oranında olmalıdır. Belirtilen varlık büyüklüğüne ulaşmak için birçok blok zincirde çok büyük miktarda maddi kaynağa ihtiyaç duyulmasına neden olur. Bu nedenle mutabakat protokolü bağlamında siber istismarın gerçekleştirilmesi pratik olarak zor bir ihtimaldir.

Genel olarak bakıldığında merkezi yazılım mimarisinin kullanılması, verinin tek merkezde saklanması ve tek merkeze güven üzerine bir yapının işletilmesi yukarıda belirtilen nedenlerden dolayı bir problemdir. Bu probleme çözüm olarak blok zincir teknolojisi ve merkezi olmayan bir mimari sunulmaktadır.

Önerilen Yöntem

Problemin tanımı başlığı altında açıklanan nedenlerden dolayı KEP sistemi için önerilen yöntem, verilerin blok zincir üzerinde saklanmasıdır. Blok zincir teknolojisi ile saklanan veriler geriye yönelik olarak değiştirilememektedir. Önerilen yöntemde veri akışı Şekil 4'te gösterildiği üzere aşağıdaki adımlardan oluşmaktadır:

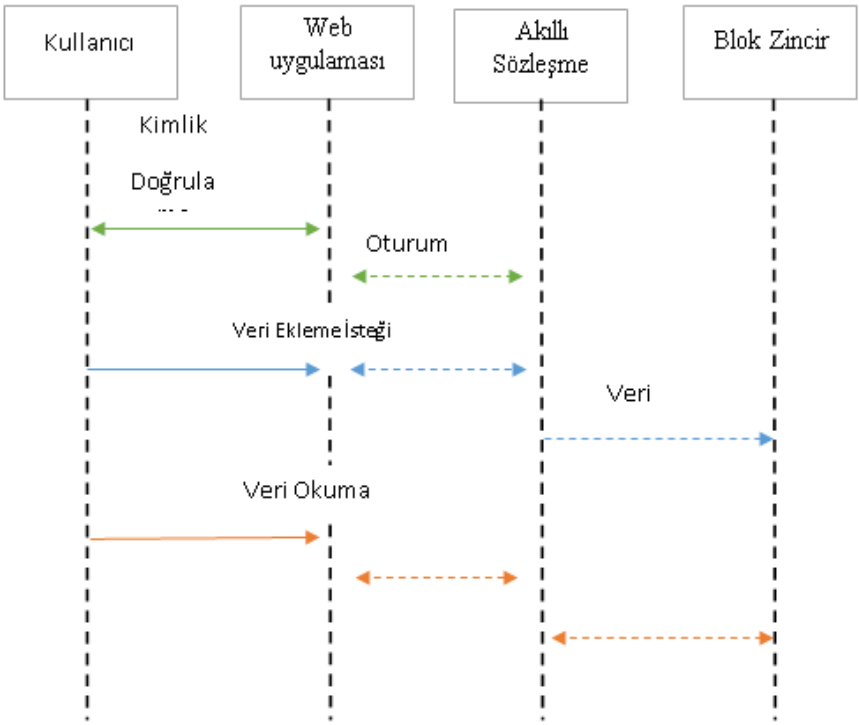
- Kullanıcı Web uygulaması üzerinden kendisine ait hesap kimlik doğrulama isteğini yollar.

- Web uygulaması akıllı sözleşmede üzerinden kimliğin oturum açıp açmayacağını kontrol eder.

- Oturum isteği başarı olması durumunda veri ekleme ve okuma yetkisi kazanır.
- Kullanıcı veri ekleme isteğini web uygulamasına gönderir. Akıllı sözleşme veri ekleme yetkisinin kontrol eder. Eğer yetki var ise blok zincir üzerine veri ekleme isteği blok zincir ağına iletilir.
- Kullanıcı veri okuma isteğinde bulunduğunda akıllı sözleşme ile yetki kontrolü gerçekleştirilir. Eğer yetkili ise veri blok zincir üzerinden çağrılır ve kullanıcıya iletilir.

Şekil 4. Veri Akış Diyagramı (Yazar tarafından çizilmiştir)

Tüm süreç kullanıcının blok zincir üzerine veri eklemesi ve okuması üzerinden



ilerlemektedir. Ancak verinin kim tarafından ekleneceği ve okunacağının kontrol edilmesi tamamen akıllı sözleşme tarafından kontrol edilmektedir. Veri akış diyagramından belirtilmemiş olan ancak bir diğer detay ise akıllı sözleşme üzerinde kontrolün kimde olacağıdır. Akıllı sözleşme akış diyagramından da anlaşılacağı üzere kullanıcı yetki veritabanı görevini yürütmektedir. Akıllı sözleşmenin en üst düzeyde yetkili olması tüm sürecin kontrolünün elinde bulundurması anlamına gelmektedir. Bu durum akıllı sözleşmenin kontrolü KEP hizmet sağlayıcıları yerine ilgili kamu kurumunda olması gerekliliğini ortaya koymaktadır.

```
// SPDX-License-Identifier: GPL-3.0
pragma experimental ABIEncoderV2;
pragma solidity ^0.8.12;
```

```
import "@openzeppelin/contracts/utils/Strings.sol";
contract messagebox{
    struct messages{
        address gonderen;
        uint mesaj_no;
        string mesaj;
    }
    struct keys{
        address gonderen;
        uint mesaj_no;
        uint mesaj_key;
    }
    struct Mesaj_list{
        address gonderen;
        uint mesaj_no;
    }

    mapping(string => keys) private keys_map;
    mapping(string => messages) private messages_map;
    Mesaj_list[] private mesaj_list;

    uint count_mesaj = 0;

    address owner;
    event Create_key(address indexed _from, uint mesaj_no, string
keymap_index, uint _mesaj_key);
    event Add_message(address indexed _from, uint _mesaj_no, string
keymap_index);
    event Mesaj_listesi(uint[] _mesaj_listesi);
    constructor(){
        owner = msg.sender;
    }

    function addressToString(address adres, uint _count_mesaj) private
pure returns (string memory) {
        return string.concat(Strings.toHexString(adres),
Strings.toString(_count_mesaj));
    }
    function genRandom(uint _count_mesaj) private view returns (uint) {
        uint random = uint(keccak256(abi.encodePacked(block.timestamp,
```

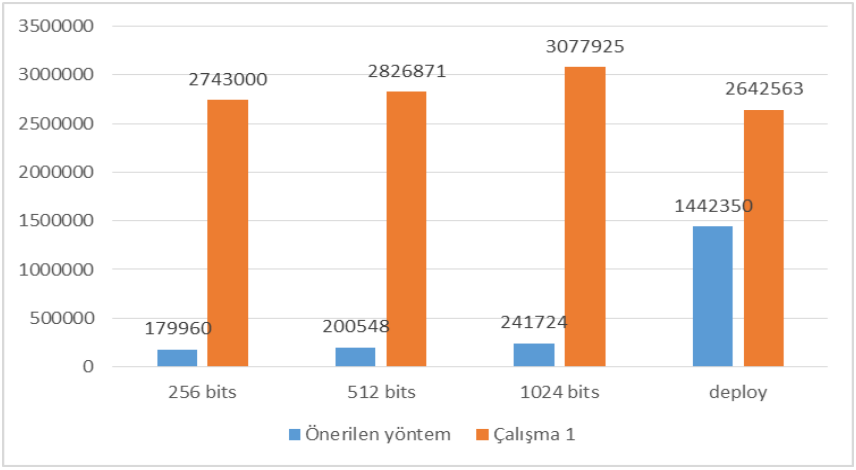
```
msg.sender, _count_mesaj))) % 100;
        return random;
    }
    function create_key() public returns(uint _mesaj_key){
        string memory keymap_index = addressToString(msg.sender,
count_mesaj);
        uint gen_random = genRandom(count_mesaj);
        keys_map[keymap_index].gonderen = msg.sender;
        keys_map[keymap_index].mesaj_no = count_mesaj;
        keys_map[keymap_index].mesaj_key = gen_random;
        emit Create_key(msg.sender, count_mesaj, keymap_index,
gen_random);
        count_mesaj++;
        return gen_random;
    }

    function add_message(string memory _mesaj, uint _mesaj_no, string
memory _keymap_index) public{
        require(keys_map[_keymap_index].gonderen == msg.sender,
"anahtar bulunamadi");
        require(keys_map[_keymap_index].mesaj_no == _mesaj_no, "mesaj
no bulunamadi");
        string memory keymap_index = addressToString(msg.sender,
_mesaj_no);
        require(messages_map[keymap_index].mesaj_no != _mesaj_no,
"mesaji degistiremezsiniz");
        messages_map[keymap_index].gonderen = msg.sender;
        messages_map[keymap_index].mesaj_no = _mesaj_no;
        messages_map[keymap_index].mesaj = _mesaj;
        mesaj_list.push(Mesaj_list({
            gonderen: msg.sender,
            mesaj_no: _mesaj_no

        }));
        emit Add_message(msg.sender, _mesaj_no, keymap_index);
    }

    function read_message(string memory _keymap_index, uint _mesaj_no)
public view returns(string memory, uint){
        require(msg.sender == owner, "yetkisiz erisim");
```

```
        require(keys_map[_keymap_index].mesaj_no == _mesaj_no, "mesaj
no bulunamadi");
        return (messages_map[_keymap_index].mesaj,
keys_map[_keymap_index].mesaj_key);
    }

    function mesaj_listesi() public returns(uint[] memory){
        require(msg.sender == owner, "yetkisiz erisim");
        uint256[] memory List = new uint256[](mesaj_list.length);
        for(uint i =0; i < mesaj_list.length; i++ ){
            List[i] = mesaj_list[i].mesaj_no;
        }
        emit Mesaj_listesi(List);
        return List;
    }


}
```

Şekil 5. Akıllı Sözleşme (Yazar tarafından geliştirilmiştir)

Akıllı sözleşmenin kendi içinde süreç yönetimi incelendiğinde create_key fonksiyonu ile veri göndermek isteyen taraf ön kayıt işlemi gerçekleştirmekte ve gönderilecek olan iletinin şifrelenmesi için anahtar almaktadır. İletinin şifrelenmesi için gerekli anahtar elde edildikten sonra mesaj eklenmesi için add_message fonksiyonu mesaj içeriği, mesaj_no ve keymap_index parametreleri ile çağrılarak mesaj eklenir. Mesajlar, read_message fonksiyonu ile sadece akıllı sözleşmeyi deploy eden tarafından okunabilmektedir.

Yapılan çalışmada geliştirilen yönteme ait akıllı sözleşme çeşitli yöntemler ile test edilmiştir ve güncel Ethereum ücreti ile fiyat verimliliği incelendiğinde kullanılabilirlik açısından değerlendirilebilir olduğu sonucunu ortaya çıkarmıştır. Geliştirilen akıllı sözleşme, kişisel kullanım ve test amacıyla kullanılan Ganache network'ü üzerinde test edilmiştir. Ganache network'ünün kullanımı, gerçek hayatta bulunan Ethereum network'ünün anlık olarak değişen ağ hızı ve maliyet sürecinden etkilenmemesini sağlamaktadır.



Şekil 6. Akıllı Sözleşme GAS Maliyet Test Sonuçları

Literatürde, tespit edebildiği kadarı ile önerilen yönteme en yakın çalışma Muit-Puigserver ve ark. tarafından geliştirilen çalışmadır. Çalışmada var olan add_message ve karşılaştırılan çalışmada bulunan createDelivery fonksiyonları temel olarak aynı işleve sahiptir. Bu fonksiyonların 256, 512 ve 1024 bit mesaj tutması sonucu harcadıkları GAS miktarı Şekil 6'da verilmiş olup akıllı sözleşmenin deploy maliyetleri karşılaştırılmıştır (Mut-Puigserver, Cabot-Nadal ve Payeras-Capellà, 2020).

Sonuç

Teknolojinin hayatın her alanında yer edinmesi artık günlük hayatın bir normali haline gelmiştir. Bu nedenle kamu hizmetlerinin teknolojiyi kullanması kaçınılmaz bir sonuçtur. Globalleşen dünyada kamu hizmetlerinin günlük hayatta var olan problemlerin çözümü noktasında yetkili merciler tarafından geliştirilen yazılım ve mimarilerin kullanışlılığı, yeknesaklığı ve güvenliği önemli hale gelmiştir. Kamu hizmetlerinin günlük hayatta var olan problemleri çözmesi amacıyla geliştirilen yazılım ve ilgili mimarilerinin kullanışlılığı ve güvenliği önemli bir problemdir. Hal böyle iken vatandaş ve kamunun daha güvenli ve verimli olabilecek şekilde iletişimin sağlanması için hayata geçirilen KEP sisteminin temel olarak çeşitli güvenlik kıstaslarına sahip olması gerekmektedir. Ancak sağlanan güvenlik tamamen KEP hizmet verenlerin kendi sunucularında var olan kapalı kutu sistemi ile ilerlemektedir. Gerekli güvenliğin sağlanıp sağlanmadığı düzenleyici kamu kurumunun denetleme yetenekleri ile sınırlıdır. Bu güvenlik politikası, yapı olarak kırılgandır. Problemin tanımında belirtildiği üzere bu politikada temel olarak 3 sorun bulunmaktadır. Birincisi, verinin tek merkezde saklanmasından dolayı verinin tutulduğu sunucunun güvenliğinin problemidir. Sunucu güvenlik istismarına uğraması durumunda veri bütünlüğünün sadece yedeklere bağlı olmasıdır. İkincisi, veri eklendiğinde sadece eklenen verinin doğruluk kontrolünden geçmesidir. Üçüncüsü, verinin değiştirilmediğinin güvencelerinden biri olan zaman damgasının tek merkezden kontrol edilmesidir.

Genel olarak değerlendirildiğinde KEP sisteminin problemlerinden olan verinin saklanmasına dair bakış açısının yeniden değerlendirilme ihtiyacı ortaya çıkmaktadır. Hali hazırda kullanılan KEP sisteminin problemlerinin genel olarak değerlendirildiğinde verinin saklanmasına dair bakış açısının yeniden değerlendirilmesi gerektiği aşikârdır.

Bu ihtiyaçtan ötürü alternatif olarak verinin kayıt altına alınması süreci için blok zincir teknolojisinden faydalanılması bir çözüm olmaktadır.

Çalışmada, KEP sisteminin âdemi merkeziyetçi yapısına alternatif olarak blok zinciri teknolojisinin entegrasyonu önerilmiştir. KEP sisteminin, veri kaydının ve onaylanmasının tek işlem birimi ve merkezde gerçekleşmesine alternatif olarak blok zinciri teknolojisinin dağıtık yapısı çözüm olmaktadır. Blok zincirinde, veri kaydı birden fazla noktada gerçekleştirilmekte ve var olan kayıtların yeterli sayıda düğüm noktası tarafından doğrulanması gerekmektedir. Bu durum, blok zinciri teknolojisi var olan problemlere sunduğu çözümlerinin yanında sistemin üçüncü tarafa olabilecek güven ihtiyacını da ortadan kalkmasını sağlamaktadır.

Hali hazırda bulunan KEP sistemleri verinin değiştirilip değiştirilmediğini kontrolünü veri paketlerinin birbirinden bağımsız bir şekilde zaman damgası ile kayıt altına alınması ile gerçekleştirmektedir. Ancak blok zinciri teknolojisi, her yeni veri bloğu oluşturulduğunda sürekli geriye yönelik veri kontrolünü gerçekleştirmektedir. Zaman damgası için gerekli zaman bilgisi blok zinciri ağında bulunan komşu düğüm noktalarından sağlanmaktadır. Bu durum veri güvenliğini parçalı değil bir bütün olarak alınmasını sağlamaktadır.

Çalışmada, blok zinciri teknolojisinin KEP sistemine entegrasyon adımları anlatılmış olup uygulama olarak gerçekleştirebileceği ortaya koyulmuştur. Çalışmada esas olan konu iletilerin güvenli olarak kayıt altına alınması ve iletinin karşı tarafa iletildiğinin reddedilemez olarak kanıtlanmasıdır. Bu yönde literatürde sadece tek bir çalışma tespit edilmiş olup, çalışmalar blok zinciri üzerinde çalışma maliyetleri karşılaştırılmıştır. Yapılan karşılaştırma sonucunda, önerilen yöntemin 256, 512 ve 1024 bit mesajlarda sırası ile %94, %93, %92 oranında daha verimli olduğu anlaşılmıştır.

Blok zinciri teknolojisi ve buna bağlı teknolojilerin günlük hayatta kullanımına yönelik çözümlerin artması ile bu teknolojinin veri kaydına yönelik getirdiği yenilik daha iyi anlaşılacaktır. KEP sisteminde de blok zincir kullanımı bir çözüm olarak değerlendirilmektedir. Bu çalışmanın sonuçları itibariyle ilgili alana ve yapılacak olan çalışmalara katkı sunabileceği düşünülmektedir. Gelecekte var olan çalışmalara ışık tutması yönüyle önerilen çözümün ilgili alana katkı sunacağı düşünülmektedir.

Değerlendirme	İki Dış Hakem / Çift Taraflı Körleme
Etik Beyan	Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur.
Benzerlik Taraması	Yapıldı – Ithenticate
Etik Bildirim	itobiad@itobiad.com
Çıkar Çatışması	Çıkar çatışması beyan edilmemiştir.
Finansman	Bu araştırmayı desteklemek için dış fon kullanılmamıştır.

Peer-Review	Double anonymized - Two External
Ethical Statement	It is declared that scientific and ethical principles have been followed while carrying out and writing this study and that all the sources used have been properly cited.
Plagiarism Checks	Yes - Ithenticate
Conflicts of Interest	The author(s) has no conflict of interest to declare.
Complaints	itobiad@itobiad.com
Grant Support	The author(s) acknowledge that they received no external funding in support of this research.

Kaynakça / References

Allison, I. (2016). Skuchain: Here's how blockchain will save global trade a trillion dollars. *International Business Times*, 1–5. https://www.ibtimes.co.uk/skuchain-heres-how-blockchain-will-save-global-trade-trillion-dollars-1540618. Erişim tarihi: 28.12.2021

Amoroso, A. (2018, September). Are E-mails Files Reliable Evidences?. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)* (pp. 32-36). IEEE.

Arslan, M., ve Biniş, M. (2016). Türk vergi sisteminde tebligat ve elektronik tebligat. *Yönetim ve Ekonomi Araştırmaları Dergisi*, *14*(1), 300-317.

Aydar, M., Cetin, S. C., Ayvaz, S., ve Aygun, B. (2019). Private key encryption and recovery in blockchain. *arXiv preprint arXiv:1907.04156*.

Bayram, M., ve Karabalık, A. (2015). E-Tebligat Ve Kayitli Elektronik Posta Sistemi Uygulamalari. *Çözüm, 128, 145-152*.

Beceriklican, N. (2019). *Türk vergi sisteminde elektronik tebligat: Eskişehir ili üzerine bir inceleme* (Master's thesis, ESOGÜ, Sosyal Bilimleri Enstitüsü).

Berber, L. K. (2009). Registered e-Mail and e-Invoicing in Turkey. *Digital Evidence & Elec. Signature L. Rev.*, *6*, 197.

Boverman, A. (2015), https://culubas.blogspot.com/. Erişim tarihi:19.02.2022

Börü, L. (2012). Elektronik Tebligat Yönetmeliği Taslağı'na İlişkin Kısa Bir Değerlendirme. *Ankara Barosu Dergisi*, (2), 403-410.

Brito, J. ve Castillo, A. (2013). BITCOIN A Primer for Policymakers. http://online.wsj.com/article/SB100. Erişim tarihi: 28.12.2021

BTK (2017), https://www.btk.gov.tr/kayitli-elektronik-posta-hizmet-saglayicilar. Erişim tarihi:09.03.2022

BTK (2017), KEP'e İlişkin Sıkça Sorulan Sorular, https://www.btk.gov.tr/kep-e-iliskin-sikca-sorulan-sorular. Erişim tarihi: 14.03.2022

Buterin V. 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Erişim tarihi: 14.03.2022

Carson B., Romanelli G., Walsh P., and Zhumaev A.. (2018). The strategic business value of the blockchain market | McKinsey. *McKinsey&Company*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. Erişim tarihi:20.01.2022.

Clack, C. D., Bakshi, V. A. ve Braine, L. (2016). Smart contract templates: foundations, design landscape and research directions. *arXiv preprint arXiv:1608.00771*.

CNIL. (2018). Blockchain. Solutions for a responsible use of the blockchain in the context of personal data. CNIL Report.Commission Nationale Informatique and Libertés. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf . Erişim tarihi:18.01.2022.

Conoscenti, M., Vetro, A., ve De Martin, J. C. (2016), "Blockchain for the Internet of Things: A systematic literature review," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1-6, doi: 10.1109/AICCSA.2016.7945805.

Conti, M., Kumar, E. S., Lal, C., ve Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4), ss. 3416-3452.

De La Rosa, J. L., Torres-Padrosa, V., El-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., ve Miralles, F. (2017, December). A survey of blockchain technologies for open innovation. In *Proceedings of the 4th Annual World Open Innovation Conference* (pp. 14-15).

Eker Kitiz, E. A. (2019), Kayıtlı Elektronik Posta Sistemi, *İstanbul Barosu Dergisi*, 93(2), 15-24.

Emam, A. H. M. (2013). Additional authentication and authorization using registered email-ID for cloud computing. *International Journal of Soft Computing and Engineering*, *3*(2), 110-113.

Enis Karaarslan, Melih Birim, "Blokzincirde Güvenli ve Güvenilir Uygulama Geliştirme Temelleri", Siber Güvenlik ve Savunma: Blokzinciri ve Kriptografi, p 1- 48, Nobel Yayınevi, 2021

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., ve Levchenko, K. (2015, October). Security by any other name: On the effectiveness of provider based email security. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 450-464).

Garfinkel, H. ve Drane, J. (2016). What is blockchain? *Splunk*, (January), 4. https://www.splunk.com/en_us/data-insider/what-is-blockchain.html. Erişim tarihi:19.01.2022.

Gaži, P., Kiayias, A. ve Russell, A. (2018). Stake-bleeding attacks on proof-of-stake blockchains. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, ss. 85–92. IEEE.

Güler, C. ve Furat, F. (2022). Belge Yönetimi ve Arşiv Uygulamalarının Bilgi Güvenliği İlkelerine Katkısı: Kavramsal Bir Değerlendirme . *Türk Kütüphaneciliği* , 36 (1) , 74-89 . DOI: 10.24146/tk.1012325

Hao, Y., Li, Y., Dong, X., Fang, L. ve Chen, P. (2018). Performance analysis of consensus algorithm in private blockchain. *2018 IEEE Intelligent Vehicles Symposium (IV)*:280–285. IEEE.

Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., ve Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060.

Hepaksaz, E., ve Hayrullahoğlu, B. (2011). E-Devlet Kapsamında Vedop Uygulamaları Ve E-Haciz. *Sosyal ve Beşeri Bilimler Dergisi*, 3(2), 109-120.

Hinarejos, M. F., Ferrer-Gomila, J. L. ve Huguet-Rotger, L. (2019). A solution for secure certified electronic mail using blockchain as a secure message board. *IEEE Access*, *7*, 31330-31341.

Hinarejos, M. F., ve Ferrer-Gomila, J. L. (2020). A solution for secure multi-party certified electronic mail using blockchain. *IEEE Access*, *8*, 102997-103006.

Jamil, F., Hang, L., Kim, K. ve Kim, D. (2019). A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics* . doi:10.3390/electronics8050505

Kandur, H. (2011). Türkiye'de kamu kurumlarında elektronik belge yönetimi: mevcut durum analizi ve farkındalığın artırılması çalışmaları. *Bilgi Dünyası*, 12(1), 2-12

Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., ve Alam, T. M. (2019, November). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. In *2019 International Conference on Innovative Computing (ICIC)* (pp. 1-7). IEEE.

Liu, M. ve Fraser, J. (2018). *Origin White Paper*. https://www.originprotocol.com/en/whitepaper. Erişim tarihi:17.01.2022.

Mikrokep (2022), KEP Nedir?, https://www.mikrokep.com.tr/tr/kep-nedir. Erişim tarihi: 14.03.2022

Mut-Puigserver, M., Cabot-Nadal, M. A., ve Payeras-Capellà, M. M. (2020). Removing the trusted third party in a confidential multiparty registered eDelivery protocol using blockchain. *IEEE Access*, *8*, 106855-106871.

Mut-Puigserver, M., Payeras-Capellà, M. M., ve Cabot-Nadal, M. A. (2018). Blockchain-based fair certified notifications. In *Data privacy management, cryptocurrencies and blockchain technology* (pp. 20-37). Springer, Cham.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nussbaum, J. (2017). Mapping the blockchain project ecosystem. *TechCrunch*. , 17 Ekim, https://techcrunch.com/2017/10/16/mapping-the-blockchain-project-ecosystem/. Erişim tarihi:20.01.2022.

O'Regan, G. (2018). Email Communication. In *The Innovation in Computing Companion* (pp. 123-126). Springer, Cham.

Organ, A., ve Karadağ, N. C. (2011). İşletmecilik Açısından Elektronik Ticaret ve Hukuki Altyapısı. *Journal of Internet Applications and Management*, 2(2), 81-104.

Öz, E., ve Bozdoğan, D. (2012). Türk Vergi Sisteminde E-Maliye Uygulamaları. *Suleyman Demirel University Journal of Faculty of Economics & Administrative Sciences*, 17(2).

Öztürk, G. (2019). *Türkiye'de e-Devlet Sürecinde Elektronik Tebligat ve Kayıtlı Elektronik Posta (KEP) Uygulaması.* Yayınlanmamış Yüksek Lisans Tezi, Hacetepe Üniversitesi, Ankara.

Paloque-Bergès, C., ve Schafer, V. (2019). Arpanet (1969–2019). *Internet Histories*, *3*(1), 1-14.

Payeras-Capella, M. M., Mut-Puigserver, M., ve Cabot-Nadal, M. A. (2019). Blockchain-based system for multiparty electronic registered delivery services. *IEEE Access*, *7*, 95825-95843.

Payeras-Capellà, M., Mut-Puigserver, M., ve Cabot-Nadal, M. À. (2018b, November).

Smart contract for multiparty fair certified notifications. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)* (pp. 459-465). IEEE.

Prasad, A. (2018). Blockchain Use Cases. *bbntimes*. 24 Haziran, https://www.bbntimes.com/technology/blockchain-use-cases . Erişim tarihi:20.01.2022.

PTT (2022), Nasıl çalışır?, https://pttkep.gov.tr/nasil-calisir/. Erişim tarihi: 14.03.2022

Rebovich, D., ve Byrne, J. M. (Eds.). (2022). *The New Technology of Financial Crime: New Crime Commission Technology, New Victims, New Offenders, and New Strategies for Prevention and Control*. Routledge.

Resmi Gazete (2011), https://www.resmigazete.gov.tr/eskiler/2011/02/20110214-1-1.htm. Erişim tarihi: 09.03.2022

Riabov, V. V. (2005). SMTP (Simple Mail Transfer Protocol). *River College*.

Rivest, R. L., Shamir, A., ve Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

Ruggieri, F. (2010). Registered e-mail (REM)—Reliable e-mail for everybody. *Datenschutz und Datensicherheit-DuD*, *34*(5), 314-317.

Samast, Y. (2014), Kayıtlı elektronik posta (KEP), *XIX. Türkiye'de internet Konferansı,* inet-tr

Sharma, A. (2018, 24 Ağustos). 5 Trends Shows How Blockchain Is Changing Social Media | Hacker Noon. *Hackernoon*. 24 Ağustos. https://hackernoon.com/5-trends-shows-how-blockchain-is-changing-social-media-ba50c975c041. Erişim tarihi: 26.11.2021

Shermis, M. D., ve Lombard, D. (1999). A comparison of survey data collected by regular mail and electronic mail questionnaires. *Journal of Business and Psychology*, *14*(2), 341-354.

Tauber, A. (2011). A survey of certified mail systems provided on the Internet. *Computers & Security*, *30*(6-7), 464-485.

Tosun, M. (2016), Kayıtlı Elektronik Posta (KEP) nedir ?, https://www.yerelbt.com/kayitli-elektronik-posta-kep-nedir/. Erişim tarihi: 14.03.2022

TSE. (2014). Elektronik doküman ve belge yönetim sistemi koruma profili (sürüm1.3.1). Ankara: Yazar. https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2231/09012015111018-3.pdf

Varol, A., ve Baştürk, İ. (2015). Hukuki ve teknik boyutuyla elektronik tebligat ile kayıtlı elektronik posta sistemi. *Ankara Barosu Dergisi*, (1).

Xue, T., Yuan, Y., Ahmed, Z., Moniz, K., Cao, G., ve Wang, C. (2018, July). Proof of contribution: A modification of proof of work to increase mining efficiency. In *2018 IEEE 42nd annual computer software and applications conference (COMPSAC)* (Vol. 1, pp. 636-644). IEEE.

Yalçınkaya, B. (2015). Elektronik belge yönetimi (EBY) uygulamalarında başarıyı olumsuz etkileyen risk unsurları. *Bilgi ve Belge Araştırmaları Dergisi*, 4, 20-40.

Yang, X., Chen, Y., ve Chen, X. (2019, July). Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In *2019 IEEE International*

Conference on Blockchain (Blockchain) (pp. 261-265). IEEE.

Ye, C., Li, G., Cai, H., Gu, Y. ve Fukuda, A. (2018). Analysis of security in blockchain: Case study in 51%-attack detecting. *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*, ss. 15–24. IEEE.

Yılmaz, Y., ve Üstündağ, M. T. (2015). Kayıtlı Elektronik Posta (KEP) hizmetinin kamu kuruluşlarına ait elektronik belge yönetimi sistemlerinde kullanılması. *Bilgi Dünyası*, *16*(2), 204-221.

Yurtsever, H. (2016). Vergi hukukunda tebligatta yeni bir uygulama: elektronik tebligat. *Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *23*(2), 451-466.

Yüce, M., ve Çelik, M. (2016). Solution Recommendations To The Problems That Can Be Faced During The Implementation Of Electronic Notification At Turkish Tax System. *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi*, 2(4), 67-79.