ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRKİYE'DE DİJİTAL DEVLET PAYDAŞLARI ARASINDAKİ ETKİLEŞİM SÜREÇLERİNDE BLOKZİNCİRİNİN KULLANILABİLİRLİĞİ

Mustafa SAYIN

Tez Danışmanı
Prof.Dr. Türksel KAYA BENSGHİR

YÜKSEK LİSANS TEZİ
AMME İDARESİ ANABİLİM DALI
GÜVENLİK YÖNETİMİ BİLİM DALI

AĞUSTOS 2022


ankara
HBM

TÜRKİYE'DE DİJİTAL DEVLET PAYDAŞLARI ARASINDAKİ ETKİLEŞİM SÜREÇLERİNDE BLOKZİNCİRİNİN KULLANILABİLİRLİĞİ

Mustafa SAYIN

YÜKSEK LİSANS TEZİ
AMME İDARESİ ANABİLİM DALI
GÜVENLİK YÖNETİMİ BİLİM DALI

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

AĞUSTOS 2022

ETİK BEYAN

Ankara Hacı Bayram Veli Üniversitesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mustafa SAYIN

11.08.2022

TÜRKİYE'DE DİJİTAL DEVLET PAYDAŞLARI ARASINDAKİ ETKİLEŞİM SÜREÇLERİNDE BLOKZİNCİRİNİN KULLANILABİLİRLİĞİ

(Yüksek Lisans Tezi)

Mustafa SAYIN

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Ağustos 2022

ÖZET

Bilgi ve İletişim Teknolojilerinin (BİT) kamu yönetimi ve hizmet sunumunda kullanılması ile başlayan süreçte, geleneksel devlet önce e-devlete, müteakiben dijital devlete dönüşmüştür. Dijital devlette, vatandaş ve paydaşların ihtiyaçlarına cevap veren birlikte çalışabilir, birbiri ile entegre olmuş, etkin, şeffaf ve basitleştirilmiş iş süreçlerine sahip bir yapılanma hedeflenmektedir. Ancak bilgi sistemleri arasındaki etkileşim süreçlerinde, teknik sorunlar, idari süreçler ve kurumların birbirinin verisini anlamlandırarak kendine uygun formata dönüştürebilmesinde zorluklar yaşanmaktadır. Blokzinciri ve onun altında yatan dağıtık defter teknolojisi, finans alanında bir teknoloji olarak ortaya çıkmakla birlikte, şeffaflık, verimlilik, veri bütünlüğü ve güvenlik gibi özellikleri ile birlikte çalışabilirlik açısından, kurumlar arasındaki etkileşim süreçlerinde uygulanabilir. Çalışma, blokzinciri teknolojisi ve dijital devlet açısından mevcut uygulama alanlarına ilişkin akademik literatürü incelemeyi, bu teknolojinin Türkiye'de dijital devlet paydaşları arasındaki etkileşim süreçlerinde kullanılabilirliğini, olası zorluk ve sınırlamaları değerlendirmeyi amaçlamaktadır. Çalışmanın yöntemi literatüre dayalı örnek olay incelemesi olarak belirlenmiştir. Öncelikle dijital devlet ve blokzinciri teknolojisinin özellikleri ve akademik literatür analiz edilmiştir. Ardından blokzinciri teknolojisine strateji ve politikalarında yer veren ve bunu pilot uygulamalarla test eden uluslararası kuruluş ve ülkeler ile Türkiye'nin mevcut durumu incelenmiştir. Analizler ışığında Türkiye'de dijital devlet bağlamında birlikte çalışabilirliğe en uygun çıkarımlar yapılarak, potansiyel zorluk ve sınırlamaları tespit edilmiştir. Çalışma, blokzinciri teknolojisinin şimdiye kadar kamu sektörü üzerinde minimum etkisi olduğunu ve Türkiye'nin de blokzincirinin kamusal alanda uygulanması açısından erken dönemde bulunduğunu; ülke örnekleri ve pilot çalışmalar, blokzincirinin etkileşim süreçlerini iyileştirmek için yeni bir yol olabileceğini göstermektedir. Bu nedenle, kavram kanıtı ve pilot çalışmaların yapılmasının önemli olduğu tespit edilmiştir. Blokzincirinin değişmezlik özelliğinin kişisel verileri ve mahremiyeti tehdit etme potansiyeli nedeniyle, uygulama alanlarının detaylı olarak düşünülmesi gerekmektedir.

Bilim Kodu : 114601
Anahtar Kelimeler : Türkiye, Blokzinciri, Dijital Devlet, Birlikte Çalışabilirlik, Paydaş.
Sayfa Adedi : 65
Tez Danışmanı : Prof. Dr. Türksel KAYA BENSGHİR

USABILITY OF BLOCKCHAIN IN INTERACTION PROCESSES BETWEEN DIGITAL GOVERNMENT STAKEHOLDERS IN TURKEY

(M. Sc. Thesis)

Mustafa SAYIN

ANKARA HACI BAYRAM VELİ UNIVERSITY

THE INSTITUTE OF GRADUATE STUDIES

August 2022

ABSTRACT

In the process that started with the use of Information and Communication Technologies (ICT) in public administration and service delivery, the traditional state first transformed into e-government and then digital government. In the digital government, a structuring that responds to the needs of citizens and stakeholders, has interoperable, integrated, effective, transparent and simplified business processes is aimed. However, there are difficulties in the interaction processes between information systems, technical problems, administrative processes and institutions in making sense of each other's data and transforming it into a suitable format. Although blockchain and its underlying distributed ledger technology emerge as a technology in the field of finance, it can be applied in interaction processes between institutions in terms of transparency, efficiency, data integrity and security, with regards to interoperability. The study aims to examine the academic literature on the current application areas of blockchain technology and digital government, to evaluate the usability of this technology in the interaction processes between digital government stakeholders and possible difficulties and limitations in Turkey. The method of the study was determined as a case study based on the literature. First of all, the features of digital government and blockchain technology and academic literature were analyzed. Then, the current situation of Turkey and international organizations and countries that include blockchain technology in their strategies and policies and test it with pilot applications are examined. In the light of the analysis, the most appropriate deductions for interoperability in the context of digital state in Turkey were made and potential difficulties and limitations were determined. The study shows that blockchain technology has had minimal impact on the public sector so far and that Turkey is in an early stage in terms of blockchain implementation in the public sphere; country examples and pilot studies show that blockchain can be a new way to improve interaction processes. Therefore, it has been found that it is important to conduct proof-of-concept and pilot studies. Due to the potential of the immutability feature of the blockchain to threaten personal data and privacy, its application areas need to be considered in detail.

Science Code : 114601
Key Words : Turkey, Blockchain, Digital Government, Interoperability, Stakeholder.
Page Number : 65
Supervisor : Prof. Dr. Türksel KAYA BENSGHİR

TEŞEKKÜR

Yüksek lisans eğitimine başladığım Türkiye ve Orta Doğu Amme İdaresi Enstitüsü (TODAİE)'de derslerini almış olduğum hocalarıma kazandırmış oldukları yeni bakış açılarından, Danışman hocam Prof. Dr. Türksel KAYA BENSGHİR'e tez konusunun belirlenmesi ve özgün içerikle kurgulanması aşamalarında kritik yönlendirmelerinden ve hiçbir zaman esirgemediği destekten dolayı eşime teşekkür ederim.

İÇİNDEKİLER

Sayfa

TABLOLARIN LİSTESİ

Tablo **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BİT	Bilgi ve İletişim Teknolojileri
dApp	Merkezsiz Uygulama (Decentralised Application)
DLT	Dağıtık Defter Teknolojisi (Distributed Ledger Technology)
DPoS	Yetkilendirilmiş Sahipliğin İspatı (Delegated Proof of Stake)
EBSI	Avrupa Blokzinciri Hizmet Altyapısı (European Blockchain Services Infrastructure)
EKAP	Elektronik Kamu Alımları Platformu
EVM	Ethereum Sanal Makinesi (Ethereum Sanal Machine)
G2B	Devletten Özel Sektöre (Government to Business)
G2C	Devletten Vatandaşa (Governmet to Citizen)
G2E	Devletten Çalışana (Government to Employee)
G2G	Devletten Devlete (Government to Government)
ICT	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
IoT	Nesnelerin İnterneti (Internet of Things)
KSI	Anahtarsız İmza Altyapısı (Keyless Signature Infrastructure)
P2P	Eşler Arası (Peer-to-Peer)
PBFT	Pratik Bizans Hata Toleransı (Practical Byzantine Fault Tolerance)
PoA	Yetkinin İspatı (Proof of Authority)
PoS	Sahipliğin İspatı (Proof of Stake)
PoW	Emeğin İspatı (Proof of Work)
SDK	Yazılım Geliştirme Kiti (Software Development Kit)
SHA-256	Güvenli Karma Algoritması (Secure Hash Algorithm)

1. GİRİŞ

Kamu yönetiminin temel amaçlarından biri, kamu hizmetlerini vatandaşlara sunmak ve toplumun değişen ve gelişen ihtiyaçlarına cevap vermektir. Teknolojideki gelişmelerle birlikte kamu yönetim sistemleri de değişmiş ve teknolojik gelişmeleri idari ve politika süreçlerine dahil etmiş, bu da geleneksel devleti, e-devlete ve dijital devlete dönüştürmüştür.

Bu dönüşüme ilave olarak, yeni kamu yönetimi anlayışı ile birlikte "yönetişim" ve "e-yönetişim" kavramları ortaya çıkmıştır. Yönetişim kavramı; kamu politikasının yapımı ve sunumu sürecine devlet dışı aktörlerin artan katılımını ifade eder (Bache, 2000:577).E-yönetişim ise yönetişim sürecinde bilgi ve iletişim teknolojilerinin önemini ön plana çıkarmakta ve bir aşama halinde e-devlete eklemlenmektedir (Yıldırım, 2010). E-yönetişim, kamu hizmetlerinin sunumunu değiştirirken vatandaş ve devlet arasındaki ilişkiyi yeniden yapılandıran teknoloji aracılıklı bir dizi süreçten oluşmaktadır. E-yönetişim, e-devletin yanı sıra kamu politikalarının şekillenmesi, tartışılması ve uygulanması sürecinde paydaşların çevrimiçi bağlantısı gibi yönetişimin anahtar konularını içermektedir (Torres, Pina ve Royo, 2005: 534- 535). Burada "paydaşlar", kamu kurumları, vatandaş, özel sektör, sivil toplum örgütleri ve çalışanları belirtmekte, bunlar arasındaki çok yönlü birlikte veya karşılıklı yönetim süreçleri ise "etkileşim" olarak ifade edilmektedir.

Dijital devlet sisteminde kamu hizmetlerinin, vatandaşların ve paydaşların ihtiyaçlarına cevap veren bütünleşik bir yapıda olması önem arz etmektedir. Diğer bir deyişle dijital devlet; birbiri ile entegre olmuş, etkin, şeffaf ve basitleştirilmiş iş süreçlerine sahip bir yapılanma gerektirmektedir. Türkiye'de kamu kurum ve kuruluşları iş süreçlerinin yönetimini, dijital devlet projeleri üzerinden yürütmekte, Dijital Türkiye Platformu üzerinden hizmetler sunmaktadır. Devlet bilgi sistemleri arası bilgi paylaşımı basit ve hızlı bir şekilde yürütülebilecek süreçler olarak görülmekte, fakat gerçekte teknik sorunlar, idari süreçler ve kurumların birbirinin verisini anlamlandırarak kendine uygun formata dönüştürebilmesinde zorluklar yaşanmaktadır. Ayrıca Dijital Devlet Platformuna entegre sistemlerin veri tabanları siber saldırıların ana hedefi haline gelmektedir.

Dijital devlet sürecinde karşılaşılan problemlerden bir tanesi de, kamu kurum ve kuruluşları arasında eşgüdüm eksikliğidir (Erdal, 2008). Eşgüdüm (koordinasyon),

kamu yönetiminin köklü sorun alanlarından biri olmakla birlikte, dijital devlet sürecinde farklı bir boyut kazanmıştır. BİT'deki gelişmeler sayesinde kamu yönetiminde teknoloji kullanımı yaygınlaşarak devlet ile vatandaşlar, özel şirketler, sivil toplum örgütleri gibi diğer aktörler arasındaki etkileşimin elektronik ortama aktarılması sağlanmış, elektronik veri paylaşımındaki kolaylıklar kurumların daha koordineli bir şekilde çalışabilmesine katkı sağlamıştır (İntepe, 2020). Ancak teknoloji sayesinde oldukça hızlı yayılan çok sayıda bilginin doğruluğunun sağlanması, siber saldırı riski gibi konular koordinasyonu negatif yönde etkileyebilmektedir. Bu noktada karşılıklı etkileşimi sağlarken riskleri en az düzeye indirebilecek çözümlere ihtiyaç bulunmaktadır.

Birçok bilim insanına göre (Burger, Kuhlmann, Richard, ve Weinmann, 2016; Wong, Chia, Kiu, ve Lou, 2020; Politou, Casino, Alepis, ve Patsakis, 2019), blokzinciri teknolojisi insanlık tarihinde yeni bir atılımdır. Bunun nedeni, blokzincirinin değişmez, şeffaf, merkezi olmayan ve güvenli bir dağıtık defter teknolojisi olmasıdır, bu nedenle dijitalleşme ile gelen sorunları çözmek için büyük bir potansiyele sahiptir. Blokzinciri teknolojisinin kamu yönetimi alanı için de uygulama potansiyeline sahip olduğu ifade edilebilir. Kamu yönetiminde uygulanmasına ilişkin çalışmalar, devletin mahremiyeti, güvenlik, yönetişim, şeffaflık ve hesap verebilirlik gibi kavramlar etrafında toplanmaktadır. Blokzincirinin şeffaflık, verimlilik, veri bütünlüğü ve güvenlik gibi özellikleri kamu sektörüne de fayda sağlayabilir. Ademi merkeziyetçilik özelliği, tüm paydaşlar için daha adil bir ortam sunarak birden fazla kurum arasındaki etkileşim süreçlerini iyileştirebilir. Aynı şekilde, birbirine tam olarak güvenmeyen veya bilgileri doğrulamak için herhangi bir merkezi otoriteye güvenmeyen taraflar arasında doğrudan, eşler arası veri yönetimine olanak sağlayabilir. Bu nedenle, blokzinciri ilgili çeşitli güç dinamiklerinden bağımsız olarak etkileşim süreçlerini iyileştirmek için yeni bir yol olabilir. Bunun sonucu olarak yönetişim yönülye devlet, özel sektör ve vatandaşlar arasındaki iletişim, etkileşim ve işbirliği artabilir ve bu taraflar karar alma süreçlerine aktif olarak katılabilirler (Kassen, 2021).

Birçok ülke, blokzinciri teknolojisi ile ilgili politikalarını şekillendirmeye ve dijital kimlik, kayıtlar, dijital para birimi, tedarik zinciri yönetimi, sağlık, eğitim gibi kamu hizmetlerine uygulanabilirliğini araştırmaya ve pilot uygulamalarla test etmeye devam etmektir. Artan ilgiye rağmen, özellikle kamu yönetiminde blokzinciri kullanımına

ilişkin çalışmalar son yıllarda ortaya çıkmıştır. Dünyada blokzinciri ile ilgili çalışmaların sayısı artmasına rağmen, Türkiye'de bu alanda sınırlı sayıda çalışma bulunmaktadır (Kıymık, 2019).

Çalışma, blokzinciri teknolojisi ve dijital devlet açısından mevcut uygulama alanlarına ilişkin akademik literatürü incelemeyi, bu teknolojinin Türkiye'de dijital devlet paydaşları arasındaki etkileşim süreçlerinde kullanılabilirliğini, olası zorluk ve sınırlamaları değerlendirmeyi amaçlamaktadır.

Çalışmanın yöntemi literatüre dayalı örnek olay incelemesi olarak belirlenmiştir. Öncelikle dijital devlet ve bu bağlamda birlikte çalışabilirlik ve eşgüdüm esasları ile Türk kamu yönetimindeki birlikte çalışabilirlik süreci incelenmiştir. Sonraki aşamada blokzinciri teknolojisinin tarihsel gelişimi, yapısı, avantaj ve dezavantajlarını kapsayan literatür taraması yapılmıştır. Ardından blokzinciri teknolojisine strateji ve politikalarında yer veren ve bunu pilot uygulamalarla test eden uluslararası kuruluş ve ülkeler ile Türkiye'nin mevcut durumu incelenmiştir. Analizler ışığında Türkiye'de dijital devlet bağlamında birlikte çalışabilirliğe en uygun çıkarımlar yapılarak, olası zorluk ve sınırlamaları tespit edilmiştir.

Çalışmanın sınırlamalarından biri, blokzincirinin yeni gelişen bir teknoloji olmasıdır. Literatürde oldukça fazla sayıda çalışma bulunmakla birlikte, bunların çoğu bilgisayar bilimi ve mühendisliği alanına aittir. Ekonomi, finans, siyaset bilimi, kamu yönetimi ve sosyoloji alanlarında da yayınlar olmakla birlikte, hesaplamalı bilim ve mühendislik alanlarında oldukça baskındır. Buna ek olarak, blokzinciri teknolojisinin yeniliği ve kamusal alanda uygulanması konusunda birçok belirsizlik bulunmaktadır. Bu nedenle kamu yönetimi alanında yapılan literatür taramasından elde edilen bulgular gelişmekte olan mevcut birkaç çalışma ile sınırlıdır.

Bu araştırmanın bir diğer sınırlılığı, ampirik analizin olmamasıdır. İncelenen pilot çalışmalar ve kavramların kanıtlanması gerçekleştirilmiştir, ancak bu çalışmaların sonuçları genellikle herhangi bir ampirik veri sağlamamaktadır. Benzer şekilde, çalışmamız Türkiye'de dijital devlet örneğine ilişkin sonuçları desteklemek için herhangi bir ampirik veri kullanmamaktadır. Türkiye'deki plan ve programlar blokzinciri ve ilgili eylemlerle ilişkili politikalara ve stratejilere işaret etmesine rağmen, kavram ispatı veya yargılama yürütmemektedir. Bu nedenle, halihazırda analiz edilecek ampirik veri eksikliği bulunmaktadır.

2. DİJİTAL DEVLET

Bu bölümde dijital devletin kavramsal çerçevesine odaklanılarak literatür taraması yapılmıştır. Bu bağlamda, birlikte çalışabilirlik, eşgüdüm, kurumlar arası bilgi paylaşımının başarılı bir dijital devlet modeli açısından önemi ve Türkiye'deki birlikte çalışabilirlik gelişimi incelenmiştir.

2.1. Dijital Devletin Tanımı

Dijital devlete ilişkin literatür gözden geçirildiğinde, "Dijital Devlet" ile birlikte "e-devlet", "e-government", "online government" ve "digital government" kavramlarına yer verildiği görülmektedir. Türkiye'de ise dijital devlet kavramı ile eş anlamlı olarak daha çok "elektronik devlet" yani "e-Devlet" kavramı kullanılmaktadır (Karagülmez, 2010:255). Bu doğrultuda çalışmanın bu bölümünde dijital devlete ilişkin kavramsal çerçeve çizilirken, "Dijital Devlet" ve "e-Devlet" eşanlamlı olarak kullanılmıştır.

Bilgi ve İletişim Teknolojilerinin (BİT) gelişimi ile ortaya çıkan e-Devlet'in literatürde pek çok tanımı yer almaktadır. En basit anlamda e-Devlet; bilgi ve iletişim teknolojilerinin kamu yönetiminde, hizmet sunumunda kullanılmasını ifade etmektedir. Daha geniş bir ifade ile devletin bilgi ve hizmetlerine erişimi, vatandaşlara, iş ortaklarına, çalışanlarına ve diğer kurumlara ulaştırılması ve bunlara erişimi artırmak için web tabanlı internet uygulamalarına ek olarak iş süreçlerinde teknolojinin kullanılması anlamına gelir.

Erdem'e (2014) göre e-Devlet; devlet, vatandaş, özel sektör ve bürokrasi arasında kurulan elektronik bağlantı ile zaman, emek ve parasal tasarruf sağlamayı amaçlayan bir yapıdır. Sadece BİT'lerin kullanımı değil, yönetim anlayışındaki değişimi ifade eden başka bir tanıma göre e-Devlet; kamusal politika geliştirme sürecini güçlendirmek suretiyle kamu hizmetlerinde etkinlik sağlamak ve demokratik süreçleri iyileştirmek için kamu idaresinde bilgi teknolojilerinin kullanımını ifade eder (Bensghir, 2008). OECD, e-Devleti "Daha iyi bir yönetim gerçekleştirmek için bilgi ve iletişim teknolojilerinin kullanımı ve özellikle internetin kullanılması" şeklinde tanımlanmaktadır. 03.09.2016 Tarihli ve 29820 Sayılı Resmi Gazete'de yayımlanan e-Devlet Yönetmeliği'ne göre e-Devlet;

> Hizmet süreçlerinin vatandaş odaklı olarak yeniden yapılandırılmasını da içerecek şekilde, kurumlar arası veri paylaşımı esasına dayalı olarak yürütülmesi için kurumlar tarafından, hızlı, güvenli, etkili, verimli, şeffaf ve hesap verebilir, temel hak ve özgürlüklere riayet edilerek ve mahremiyet gözetilecek şekilde elektronik ortama aktarılan her bir kamu hizmeti

şeklinde tanımlanmıştır.

Literatürde yer alan tanımları artırmak mümkündür. Ancak çalışmanın amacı bu tanımlara yer vermekten ziyade, e-Devlet'in içerdiği öğelerden yola çıkarak esas olarak barındırdığı unsurları açıklamaktır. Bu çerçevede Sobacı (2012) e-Devleti şu şekilde tanımlamıştır:

> Kamu hizmetlerinin etkin, verimli, erişilebilir ve yaygın bir şekilde sunulması; kamu kurumları arasındaki iş birliği ve bilgi bütünlüğünün sağlanması suretiyle yönetsel süreçlerin geliştirilmesi; vatandaşlar, özel sektör ve diğer paydaşlarla iletişimin kolaylaştırılması ve demokratik değer ve uygulamaların teşvik edilmesi için BİT'lerin ve özellikle internetin kamu kurumları tarafından kullanılmasıdır. (s.8)

2.2. Dijital Devlette Etkileşim Alanları

Çeşitli yönetim biçimleriyle genel bir kamu hizmeti sunum sisteminin sağlanması, çok çeşitli paydaşlara hitap eder. Etkileşimin merkezinde devletin bulunduğu dijital devlet yapısında, paydaşlar, vatandaşlar (G2C – Devletten Vatandaşa), işletmeler (G2B – Devletten İşletmeye); diğer hükümetler, devlet daireleri ve kurumları (G2G – Devletten Devlete); çalışanlar (G2E – Devletten Çalışanlara) olarak sınıflandırılmaktadır (Caldow, 2004; Christensen ve Lægreid, 2007).

2.2.1. Devlet Vatandaş Etkileşimi

Devlet Vatandaş Etkileşimi (Governmet to Citizen-G2C) genellikle vatandaş merkezli olarak kabul edilir ve temel özelliği, devlet hizmetlerine vatandaşların internet üzerinden erişmesidir. Birden fazla kanal ve web sitesi kullanımı yoluyla devlet, bilgi ve hizmetleri vatandaşları için daha erişilebilir hale getirerek, hükümet ile vatandaş arasında kolaylaştırılmış etkileşimi sağlar (Fang, 2002 s.7). Bu modelin temel amacı, "tek noktadan alışveriş" modeline dayalı elektronik hizmetlere erişim sağlamaktır, bu modelle ilgili olarak hükümet seviyelerindeki tüm hizmetler ve işlevler hangi kurumların önerdiği fark etmeksizin vatandaşların ihtiyaç duydukları her türlü hizmete her an ulaşabilmeleri için tek bir portal içerisinde entegre edilerek sunulmaktadır.

(Alshehri ve Drew, 2010, s.36) Türkiye'de Dijital Devlet Platformu, bakanlıkların ve yerel yönetimlerin bireysel web siteleri, Türkiye'de G2C yaklaşımının bilinen örnekleridir.

2.2.2. Devlet Özel Sektör Etkileşimi

Devlet Özel Sektör Etkileşimi (Government to Business-G2B), devlet ve ticari kurumlar arasındaki iletişimi kolaylaştırabilen bir etkileşimdir. Devlet ile ticari şirketler arasındaki bağlantı, her ikisi için de hayati öneme sahip olabilir. Ticari şirketler açısından belirli bir hizmetin yerine getirilmesi için gereken süreyi ve maliyeti azaltması, tasarruf sağlarken, devlet politikalarının ve yasalarının tüm güncellemelerinin özel sektöre aktarılmasını kolaylaştırır. Başvuru formlarını indirmek, yeni lisans almak veya lisansları yenilemek G2B'nin sağlayabileceği hizmet türlerine örnektir. Bu kategorinin en popüler türlerinden biri de devletin çevrimiçi süreçler yoluyla mal ve hizmet tedarik ettiği e-tedariktir. Elektronik Kamu Alımları Platformu (EKAP), devletin tüm ihale süreçlerinin esas ve usullerinin bilgi iletişim teknolojileri imkânlarıyla desteklenmesi için 5812 sayılı kanun ve 4734 sayılı kanun kapsamında geliştirilen portalin adıdır.

2.2.3. Devlet Devlet Etkileşimi

Devlet Devlet Etkileşimi (Government to Government-G2G) etkileşimi, bilgi ve iletişim teknolojilerinin kullanılarak, farklı yönetim kademelerindeki (merkezi, bölgesel ve yerel) veya aynı kademedeki kamu kurumları arasından hizmetlerin etkileşimini ve sağlanmasını ifade eder. Kurumları arasındaki işbirliği, koordinasyon, bilgi ve belge akışı için gerekli ağ sistemi G2G uygulamalarına dahildir. Bu etkileşim kurumlar arası ve kurum içi ilişki, çaba ve kaynakların tekrarlanmasından kaçınmayı sağlar (Christensen ve Lægreid, 2007). Dijital devletin uygulanmasıyla geliştirilen birlikte çalışabilirlik çerçeveleri, kamu kurumlarının manuel yöntemlerle paylaşımı mümkün olmayan kaynakları paylaşabilmesini sağlayarak daha hızlı ve kaliteli bir karar alma ortamı yaratır. G2G, ulusal, eyalet veya il ve yerel yönetimden paydaşların ve koordinasyon yetkililerinin faaliyetlerini içerir (ITU, 2008).

2.2.4. Devlet Çalışan Etkileşimi

Devlet Çalışan Etkileşim (Government to Employee-G2E) hizmetleri, G2C hizmetlerinin yanı sıra, çevrimiçi eğitim portalları gibi insan kaynaklarının geliştirilmesi ve eğitiminin düzenlenmesi dahil, yalnızca çalışanları hedefleyen belirli hizmetleri içerir. G2E hizmetleri bürokratik işlevlerin verimliliğini artırır, hizmet sunumlarının etkin bir şekilde koordinasyonunu sağlar ve böylece iş süreçlerinin etkinliğini artırır. Bu, iç iletişimleri ve G2E, özellikle çalışanlara yasa ve yönetmelikleri anlamalarına yardımcı olabilecek hizmetler sağlar; dahası, bu tür bir hizmetin sağlanması, idari süreci geliştirebilir, belirli bir hizmeti tamamlama süresini kısaltabilir ve belirli bir süreçten sorumlu çalışan sayısını azaltabilir.

2.3. Dijital Devlet ve Birlikte Çalışabilirlik

Dijital devlet sürecinin en önemli niteliklerinden biri, bilginin diğer devlet kurumları, iş dünyası ve kar amacı gütmeyen kuruluşlar arasında paylaşılması ve entegre edilmesi olarak kabul edilir.

Yasal çerçevesi belirlenmiş sınırlar içerisinde, arka planda kurumlar arası etkileşimin sağlandığı ve vatandaşa dönük yüzünde tek bir organizasyonmuş gibi davranabilen modern ve bütünleşik e-devlet yapısı, birbiriyle uyumlu, birlikte çalışabilir, etkileşimli, izlenebilir, güvenli, güvenilir ve denetlenebilir bilgi sistemlerine ihtiyaç duyar. Bilginin kurumlar arasında ve bilgi sistemlerinde kullanılabilme ve transfer edilebilme yeteneği olarak açıklanabilecek birlikte çalışabilirliğin en geniş kapsamdaki tanımı, etkin bilgi paylaşımıdır. (T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi, 2012)

Avrupa Birlikte Çalışabilirlik Çerçevesi'nde Birlikte Çalışabilirlik; "tümüyle farklı yapılarda ve çeşitlilikte olan organizasyonların (kamu idarelerinin) destekledikleri iş süreçleri üzerinden ilgili bilgi ve iletişim teknolojileri aracılığıyla bilgi ve birikimlerini paylaşarak karşılıklı fayda sağlama ve ortak hedeflere doğru ilerleyebilme becerisi" olarak tanımlamıştır (Eroğlu, Çakmak ve Külcü, 2015).

Birlikte çalışabilirlik ihtiyaçları teknik, organizasyonel ve anlamsal olmak üzere üç boyutta incelenebilir. Teknik boyutta farklı uygulamalar arasında bilgi paylaşımını mümkün kılacak teknolojilere odaklanılırken, organizasyonel boyut teknolojilerden

çok süreç modelleme dilleri, nesneye dayalı yazılım mühendisliği gibi mühendislik metodojilerine dayalıdır. Organizasyonel birlikte çalışabilirlik kapsamında, kurumlara ait iş süreçlerinin ilişkili diğer kurumları da içerecek şekilde modellenmesiyle ilgilenilir ve kurumların amaçları ile teknik altyapıyı şekillendiren uygulama ve sistemler arasında bütünlük sağlar. Diğer bir ifadeyle, paylaşılan bilginin daha etkin olarak değişimini sağlayacak şekilde oluşturulmuş iş süreçleri ve buna uygun kurumsal yapılanma hedeflenir. Ayrıca, süreçlerin yeniden mühendisliği, kurum içi ve kurumlar arasında iş akış yönetimi, süreç ve hizmetler için ihtiyaçların belirlenmesi gibi konuları içerir. Anlamsal birlikte çalışabilirlik kapsamında ise verinin, onu üreten kurumun dışındaki kurumlar tarafından da doğru şekilde anlaşılması ve yorumlanmasına yönelik çalışmalar yer alır. (T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi, 2012)

e-Devlet'te özellikle ardışık hizmetlerin olabildiğince bağımsız, ancak bütünleşik ve tek nokta hizmetiymiş gibi kesintisiz ve tutarlı yapılması önemlidir. Bu ve benzeri e-Devlet hizmetlerinin başarıyla yürütülebilmesinin en önemli ön koşulu ise, kurumlar arasında bir "Uyuşum Çerçevesi"nin varlığı olarak karşımıza çıkmaktadır. Uyuşum, sadece teknolojilerin birlikteliği ile veri/bilgi değişimi/paylaşımı anlamına gelmemektedir. Süreçlerin, yönetim modellerinin, stratejilerin ve politikaların da uyumlu hale getirilmesi önemlidir. (Karakaya ve diğerleri, 2004)

Birlikte çalışabilirlik tanımları genellikle birlikte çalışabilirliğin alt kategori tipine dayanır; daha teknik bir bakış açısı, teknolojik standartlara dayalı olarak birlikte çalışan sistemleri vurgularken, örgütsel bakış açısı, teknik seviyenin kuruluşların bazı iş kuralları altında birlikte çalışabilmesi için bir adım olarak kullanıldığı daha yüksek seviyelere odaklanır. Birlikte çalışabilirlik kapsamı, bir Bakanlık Genel Müdürlükleri gibi alt kuruluşların aynı çatı altında olduğu alt seviyeye veya uluslararası birlikte çalışabilirlik olarak aynı proje veya amaç üzerinde çalışan farklı ülkelerin üst seviyeye kadar uzanabilir.

Organizasyonel birlikte çalışabilirliğin yaygın olarak kabul gören tanımları, organizasyonların, farklı coğrafi bölgeler ve kültürler arasında, çok farklı altyapılar üzerinde çeşitli farklı bilgi sistemlerini kullanıyor olsalar bile, anlamlı verileri (bilgileri) etkili bir şekilde iletme ve aktarma becerisi olduğunu belirtir. Kurumsal veri ve bilgiler, e-Devlet sistemleri geliştirilerek ve etkin bir şekilde kullanılarak dijital

ortamda depolanır ve paylaşılır. Organizasyonel birlikte çalışabilirliğin başarısı, planlama, uygulama ve uygulamadan başlayarak herhangi bir devlet kurumu tarafından yürütülen e-Devlet projesinin başarısı ile ilişkilidir. İşlenen ve sahip olunan veri ve bilgilerin oranı, arka ofis süreçlerinden otomasyon sistemlerine ve karar destek sistemlerine kadar dijital forma dönüştürüldüğünden, organizasyonel birlikte çalışabilirlik sürecinin bir parçası olarak bilgilerin diğer devlet kurumları ile paylaşılması daha mümkün hale gelmektedir.

Teknik, organizasyonel ve anlamsal boyutta iyi tasarlanan birlikte çalışabilirlik altyapısı, farklı kurumlar tarafından sunulan hizmetleri birbirine bağlayarak, başta vatandaşlar olmak üzere tüm paydaşlar için tek seferlik, kapsamlı çevrimiçi hizmetler sağlar. Örneğin adalet sistemi (polis, savcılar, kamu avukatları, mahkemeler, hapishaneler) altındaki çeşitli kurumların bilgi sistemleri verileri paylaşabildiyse, adalet yönetimi daha hızlı ve etkili olacaktır.

Birlikte çalışabilirlik aynı zamanda kurumların kendi iç süreçlerini daha ekonomik yönetebilmelerini de sağlayabilmektedir. Dijital toplumun doğal yapısı gereğince iş süreçleri her geçen gün değişmekte, bu da bilgi ve iletişim teknolojilerinin iş süreçlerine paralel olarak yenilenmesini zorunlu kılmaktadır. İşte birlikte çalışabilirlik, daha fazla ve daha iyi bilgi almak ve daha iyi hizmetler sunmak için daha fazla donanım ve yazılım satın alma ihtiyacını da ortadan kaldırır.

Kamu kurumları ve vatandaşlar arasında e-Devlet şemsiyesi altında birlikte çalışabilirliğin uygulanması ile ortaya çıkan gelişmiş bilgi akışı, şeffaflığı ve hesap verebilirliği de artırır. Böylece, ulusal düzeyde, birlikte çalışabilirlik iyi yönetişimi sağlayarak e-Devlet'in temel hedeflerine ulaşmada önemli katkıda bulunur.

e-Devlet'te etkin bilgi paylaşımı veriyi dijital ortama aktararak diğer kurumlarla gönderme-alma şeklinde gerçekleşmekten öte, standartları ve mimarisi iyi tasarlanmış otomatik olarak işleyen, başta kişisel verilerin korunması olmak üzere her türlü siber güvenlik önlemleri alınmış, daha iyi yönetişim için zemin oluşturan birlikte çalışılabilir bir altyapı kurmayı hedeflemelidir.

Ayrıca yukarıda bahsedilen tüm esaslara öncülük edecek husus "hukuki altyapının" oluşturulmasıdır. Bu konuda geleneksel mevzuat oluşturma bakış açısı ile yerine, etkin bilgi paylaşımını hedefleyen, kurumların bilgi paylaşımında daha istekli olmasını

sağlayan bir hukuki çerçeve, e-Devlet kapsamında birlikte çalışabilirliği tesis etmede en önemli adım sayılabilir.

2.4. Dijital Devlet ve Eşgüdüm

"Belli bir amaca ulaşmak için türlü işler arasında bağlantı, ilişki, düzen ve uyum sağlama" (TDK, 2019) olarak tanımlanan ve temel yönetim işlevlerinden (POSDCoRB) birisi olan eşgüdüm (koordinasyon), kamu kurumları arasında yetki alanlarının işbirliği içinde yürümesini sağlayan araç ve mekanizmalar olarak kabul görmekte ve bu araçların politika ve uygulama arasında tekrarlamaları, boşlukları, çelişkileri azaltmak ve daha fazla uyum yaratmak amacıyla kullanıldığı varsayılmaktadır (Bouckaert, Peters ve Verhoest, 2010: 16).

Dijitial devlet, yatay koordinasyon ve etkileşim yapısı ile ilgili ağ yapılarına dahil olan tüm tarafların katılımını öngören, bilgi ve iletişim teknolojileriyle gelişen merkezi olmayan iletişim ağlarını kullanan bir modeldir (Yılmaz, 2007). BİT sayesinde ortaya çıkan bilginin üretilmesi, toplanması, depolanması, analizi ve paylaşımı gibi imkanlar ile koordinasyona ilişkin sorunlar için yeni çözüm yolları geliştirilmeye başlanmış ve kurumiçi ve kurumlararası koordinasyon daha kolay hale gelmiştir (Snellen, 2002: 183).

Dijital devlet modeli bir ağ sisteminin üstüne kurulmaktadır. Aynı ağ sisteminden faydalanan kurumlar, işletmeler ve vatandaşlar için eşgüdüm ihtiyacı ortaya çıkmaktadır (Kırçova, 2003). Bu ağın ilişkilerinin boyutu da dijital devletin olgunlaşma düzeyini belirlemekte, bu nedenle çok taraflı bir etkileşim beklenmektedir.

Dijital devlet paydaşları arasında eşgüdümün sağlanmasında etkin bilgi paylaşımı önem arz etmektedir. Farklı kamu ve özel sektör kuruluşlarının elektronik veri tabanlarda yer alan farklı amaç ve içeriklere sahip kayıtların paylaşımı eşgüdüm ile mümkün olabilir. Elde edilen eşgüdüm sayesinde kamu kurumlarının veri sistemlerindeki bilgi dağınıklığı ve karmaşasının geçilebilir.

Teknoloji sayesinde oldukça hızlı yayılan çok sayıda bilgi, kimi zaman gerçek bilginin gölgede kalmasına neden olabilmekte, ayrıca devletin dijital ortama geçmesi de siber saldırılar gibi daha büyük riskleri de beraberinde getirmekte ve tüm bu durumlar da koordinasyonu negatif yönde etkileyebilmektedir (Mergel, Schweik ve Fountain,

2009). Bu noktada karşılıklı etkileşimi sağlarken riskleri en az düzeye indirebilecek çözümlere ihtiyaç bulunmaktadır.

2.5. Türkiye'de Birlikte Çalışabilirlik Çalışmaları

Ülkemizde kamu kurum ve kuruluşları arasında etkin ve güvenli bilgi paylaşımı amacıyla birlikte çalışabilirliğe imkân sağlayan güvenli bir altyapı kurulması hedefi ise ilk defa somut olarak 2003 yılında başlatılan e-Dönüşüm Türkiye Projesi'nde yer almıştır. E-Dönüşüm Türkiye Projesi kapsamında; başta kamu kurum ve kuruluşları olmak üzere, kamuya elektronik ortamda hizmet sunan tüm kuruluşlar arasında birlikte çalışılabilirliğin sağlanması ve bu çerçevede; yetki ve sorumluluklar, esas ve prensipler, yöntem ve kriterler ile teknik standartların belirlenmesi amacıyla 2005 yılında "e-Dönüşüm Türkiye Projesi: Birlikte Çalışabilirlik Esasları Rehberi" hazırlanmıştır. (Kalkınma Bakanlığı, 2012).

Türkiye'de birlikte çalışabilirlik açısından önemli bir gelişme olan Birlikte Çalışabilirlik Esasları Rehberi içeriği incelendiğinde genel esaslar ve birlikte çalışabilirlik politikası; bilginin sunumu, taşınması, değişimi, entegrasyonu, güvenliği ve geliştirilen çözümlerin yaşam döngülerine ilişkin teknik standartlar ve sonraki dönemde yürütülmesi öngörülen rehberi tamamlayıcı nitelikteki çalışmalar olarak üç bölümden oluştuğu görülmektedir. Rehber ayrıca Teknik Standartlar bölümünde altı temel konuda esaslar ve kullanılacak standartlar belirleyerek kurumlara yol gösterici nitelik taşımaktadır. Bu standartlar genel hatlarıyla dosya sunumu ve değişimi, ara bağlantı, veri entegrasyonu ve içerik yönetimi, güvenlik, coğrafi bilgi sistemleri ve bilgi sistemlerinin geliştirilmesi ve yönetimidir. Rehberin e-devlet hizmetlerinin sunumunda kamu kurum ve kuruluşlarının birlikte çalışabilirliğinin temelini oluşturup, arka ofis entegrasyonunun sağlanmasını kolaylaştırarak e-Devlet Kapısının etkinliğini artırdığı ifade edilmektedir (Kalkınma Bakanlığı, 2012).

Birlikte çalışabilirlik kapsamında başlatılan diğer bir çalışma ise KamuNet'dir. KamuNet'e ilişkin çalışmalar ilk olarak Ulusal Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 9'uncu maddesi (Kamu güvenli iletişim kurallarının belirlenmesi) ile başlanmıştır. 20 Ekim 2012 tarih ve 28447 sayılı Resmi Gazete`de yayımlanan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" gereğince oluşturulan "Siber Güvenlik Kurulu"nun

20 Haziran 2013'de vermiş olduğu karar ile Kamu VPN-Sanal Özel Ağlar model olarak seçilmiştir. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından KamuNet için Türk Telekom altyapısının kullanılması kararlaştırılarak 25 Şubat 2015 tarihinde protokol imzalanmıştır. Müteakiben kamu kurumlarının KamuNet ağına dahil olunması talimatı 2016/28 sayılı Başbakanlık Genelgesi 3 Aralık 2016 tarihinde Resmi Gazete'de yayımlanmıştır. "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ" ise; 21.06.2017 tarihinde Resmi Gazete'de yayımlanmıştır. (T.C. Ulaştırma ve Altyapı Bakanlığı Bakanlığı, t.y.)

Başbakanlık Genelgesinde (2009), KamuNet'in amacı;

> ….kamu kurum ve kuruluşları arasındaki veri iletişiminin kamu tarafından yeni güvenli bir altyapı sağlanıncaya kadar, kurumlar arası veri iletişiminin, internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin azaltılması, kurumlar arası iletişimde standart sağlanması, ortak uygulamalar için uygun alt yapının oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi, e-Devlet uygulamalarının güvenli olarak ortak kullanılabilmesi, kamu kurumları arasında mevcut durumda internet üzerinden gerçekleştirilen bulut uygulamalarının internetten bağımsız daha güvenli olarak sağlanması...

şeklinde belirtilmiştir.

KamuNet'in; birinci aşamada, kamu kurum ve kuruluşlarının kriptosuz olarak ağ bağlantılarının tamamlanması, ikinci aşamada, diğer güvenlik tedbirlerinin uygulandığı kriptolu iletişimin gerçekleştirilmesi şeklinde iki aşamada teşkil edilmesi planlamıştır.

KamuNet'e ilk aşamada merkezi yönetim başkent teşkilatı ve hizmet yönünden yerinden yönetim kurum ve kuruluşlarını kapsayan 99 kurum ve kuruluşun dahil edilmesi planlanmıştır.

Genelge, tebliğ ve yayımlanan diğer rehberler incelendiğinde, kamu kurumlarının sanal ağa dahil olmasına ilişkin genel esaslar ve daha çok teknik altyapı ile ilgili esasların ortaya koyulduğu görülmektedir. Bu nedenle KamuNet üzerinde verilecek hizmetlerin tamamen kurumların yetkisinde olup, sadece bir altyapı hizmetini hedeflemektedir.

Teknik ilke ve tedbir olarak yayımlanan esaslar, veri paylaşım hedefleri, hedeflerin gerçekleşmesi için tanınan süre, başarısızlık kriterleri, başarısızlık halindeki yaptırımlar ve alternatif uygulamaları içermemiştir.

e-Devlet'in önemli bir bileşeni olan kamu kurumları arasında veriyi paylaşma ve bütünleştirme yeteneklerinin geliştirilmesine yönelik, 2016-2019 e-Devlet Stratejisi ve Eylem Planında "Ortak BT Altyapıları Geliştirilecektir" şeklinde hedef konmuştur. (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2015). Bu hedefin alt eylemlerine "Kamu Entegre Veri Merkezlerinin Kurulması ve Uygulamaya Alınması: e-Devlet hizmetlerine ilişkin kurum / kuruluşlarda ayrı olarak işletilen sunucular, ana bilgisayarlar, ağlar, portaller, haberleşme hizmetleri başta olmak üzere bilgi teknolojileri altyapılarının kamu entegre veri merkezlerinde birleştirilmesi için bir altyapı oluşturulacaktır.", "Elektronik Veri ve Belge Paylaşım Altyapılarının Oluşturulması: Kamu kurum/kuruluşlarının, tek bir nokta üzerinden diğer kurum/kuruluşların yönettiği verileri yetkileri dahilinde sorgulayabilmelerini sağlayacak teknik bir altyapı kurulacaktır. Bilgi güvenliği esasları da dikkate alınarak, belirlenen öncelikli sistemlerin bu altyapıya entegrasyonu sağlanacaktır." şeklinde yer verilmiştir.

Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte 10 Temmuz 2018 tarihli ve 30474 sayılı R.G.'de yayımlanan 1 sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi kurulmuştur. Ulaştırma ve Altyapı Bakanlığında bulunan e-Devlet hizmetlerine ilişkin planlama, koordine, yürütme, izleme ve düzenleme yapma yetkisi, 24/10/2019 tarih ve 30928 sayılı Resmi Gazetede yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesi ile yürürlükten kaldırılmış ve aynı kararname ile Dijital Dönüşüm Ofisinin yetkileri artırılarak "Dijital Türkiye (e-Devlet) hizmetlerinin sunumuna aracılık etmek, kurumlar arası işbirliğini artırmak ve bu alanlarda koordinasyonu sağlamak" görevleri verilmiştir. Bununla birlikte "e-Devlet Kapısı" "Dijital Türkiye Platformu" ismini almıştır. (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, t.y.)

Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin "Dijital Türkiye Projesi" kapsamında amacı "Dijital Türkiye Platformunda katma değeri yüksek hizmet sayısını artırmak, bu hizmetlerin kapsamını genişletmek ve kullanıcı dostu ara yüzler hazırlayarak vatandaşların Dijital Türkiye Platformunu kullanımını kolaylaştırmaktır." şeklinde

ifade edilmektedir (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, t.y.). Yine diğer bir proje olan KamuNet, "Kamu kurum ve kuruluşları arasında ihtiyaç duyulan veri iletişiminin, internete kapalı ve daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin azaltılması amacıyla oluşturulmuş bir ağdır." şeklinde tanımlanmıştır. Her iki projede de kurumlar arasındaki etkileşim ve birlikte çalışabilirlik esaslarına yer verilmemiştir.

Ayrıca birlikte çalışabilirlik konusu T.C. Sanayi ve Teknoloji Bakanlığının 2023 hedeflerinde

> Teknolojilerde olduğu gibi kamu hizmetlerinde de farklı bakanlık ve birimlerin birlikte çalışması; kamudan hizmet alan vatandaşa çözüm odaklı ve proaktif bir yaklaşımla her kanaldan aynı bilgi ve hızla destek olması gerekmektedir. Sanayi ve teknoloji konularında sanayici, tedarikçi, girişimci, araştırma altyapıları ve üniversitelere 'paydaş odaklı' bir yaklaşımla tek noktadan destek ve hizmet sunmak için ilk muhatabı Sanayi ve Teknoloji Bakanlığı olacak şekilde yeni mekanizma ve yapılar kurgulanması, süreçlerin revize edilerek verimliliğin artırılması amaçlanmaktadır.

şeklinde yer bulmuştur (T.C. Sanayi ve Teknoloji Bakanlığı, 2019).

Bu bölümde dijital devlet kavramı ve kuramsal çerçevesi ele alınmıştır. Bu amaçla, birlikte çalışabilirlik ve paydaşlar arası bilgi paylaşımının başarılı bir dijital devlet modeli açısından önemi ve Türkiye'deki birlikte çalışabilirlik gelişimi analiz edilmiştir. Sonraki bölümde Blokzinciri Teknolojisi incelenmiştir.

3. BLOKZİNCİRİ TEKNOLOJİSİ

3.1. Dağıtık Defter Teknolojisi

Dağıtık defter teknolojisi (Distributed Ledger Technology-DLT), verilerin farklı düğümler (katılımcılar) arasında dağıtıldığı dijital işlemlerin kayıtlarını tutan ve üçüncü bir taraf/merkezi otoriteye ihtiyaç duymadan fikir birliği temelinde her bir düğümde eş zamanlı olarak güncellenen bir veritabanıdır. DLT, her biri tam olarak aynı veri kayıtlarına sahip olan ve düğümler olarak adlandırılan dağıtık bir bilgisayar sunucuları ağı tarafından toplu olarak sürdürülen ve kontrol edilen birden çok veri deposu (defterler) arasında veri kaydetme ve paylaşmaya yönelik yeni ve hızlı gelişen bir yaklaşımı ifade eder. Temel olarak, ağdaki her eş işlemleri işler, sonuçlar üzerinde sonuca varır ve sonuçları, fikir birliği oluşturmak için kalan eşlere yayınlar. Konsensüs sağlandıktan sonra, tüm defterler buna göre güncellenir, böylece defterler birbirinin tutarlı bir kopyasına sahip olur. Dinamik dağıtım özelliği, geleneksel bir veritabanından ve bulut bilişimden farklı olduğu yerde belirgin bir farktır, bu nedenle kontrol etmek için tek bir varlığa/yetkiye değil, ağ katılımcısının bir kısmına veya tamamına ihtiyaç yoktur. Bu ayrıca bize hiçbir varlığın kayıtları geriye dönük olarak değiştiremeyeceğini veya yeni eklemeler yapamayacağını, bunun için fikir birliğine ihtiyaç duymasını da sağlar.

Dağıtık defterler blokzinciri ve akıllı sözleşmelerden oluşur. DLT gelişen bir teknoloji olduğundan, tanımların terminolojisi yetkililer tarafından oluşturulmamıştır ve bu nedenle teknolojiden bahsederken "DLT" ve "blokzinciri" terimleri sıklıkla birbirinin yerine kullanılmaktadır. Bununla birlikte, blokzinciri bir DLT'dir, ancak DLT mutlaka bir blokzinciri değildir.

Blokzinciri genellikle Dağıtık Defter Teknolojisi (DLT) olarak sınıflandırılır. Kriptografiye dayalı, paylaşılan, dağıtık, kopyalanabilir, eşzamanlı olarak erişilebilir, mimari olarak merkezi olmayan bir defter kullanan bir dizi teknoloji ve protokolden oluşur. Hem açık metin hem de şifreli olarak verilerin kaydedilmesine, doğrulanmasına, güncellenmesine ve depolanmasına izin verir. Defterin bütünlüğü her katılımcı tarafından doğrulanabilir ve değiştirilemez (Xu, Weber ve Staples, 2019)

En önemli özellikleri arasında dağıtık defter kavramı temeldir. Defter terimi ile önceden tanımlanmış bir yapıya göre bilginin depolandığı dijital bir belgeyi

kastedilmektedir. Başka bir deyişle, defter, burada yukarıda açıklanan veri tabanı kavramına atıfta bulunur. Bununla birlikte önemli fark bu tür bir veri tabanının merkezi olmayan yapıya sahip olmasıdır.

DLT tarafından kullanılan veri tabanının dağıtık yapısı, her katılımcının bulunduğu bir ağda paylaşıldığı anlamına gelir ve her düğüm normalde defterin bir kopyasını tutar. Merkezi sistemlerle ilgili dikkate değer fark, bu durumda bu tür kopyaların yalnızca yedekleme olmamasıdır. Veritabanının depolandığı her düğüm, dağıtık ağdaki diğerleriyle aynı yetkiye sahip olabilir. Genel bir kural olarak, pasif veya ikincil düğümler yoktur. Bu, defterin içeriğinin mükemmel şeffaflığına izin verme ve tek bir hata noktasından kaçınmanın çifte avantajına sahiptir.

DLT'lerin kamu idareleri için önemli bir özelliği, ağın genel veya özel olabilmesidir. Herkese açık blokzincirilerinde, herkes dağıtık defterin tamamını kendi cihazında depolayabilir ve böylece ağda tam bir düğüm haline gelebilir. Özel olanlarda, aksine, yalnızca bunu yapmaya yetkili olanlar deftere erişebilir.

Bir diğer önemli fark, izinli ve izinsiz DLT sistemleri arasındadır. İlki, tüm kullanıcıların dağıtık defterde depolanan veriler üzerinde aynı güce sahip olmadığı bir kimlik doğrulama sistemine dayanmaktadır. İkincisi, bunun yerine herhangi bir kimlik doğrulama önleminden yoksundur, böylece ağın kendisi tarafından bunu yapmak için belirlenen kurallara uyması halinde, kayıt defterinde saklanan veriler üzerinde herhangi bir işlem gerçekleştirilebilir. (Wüst ve Gervais, 2018)

Blokzinciri teknolojilerinin dayandığı defterin dağıtık yapısı, verilerin kriptografik bir temelde kaydedilmesi, doğrulanması, güncellenmesi ve depolanmasını yönetme ihtiyacının temelini oluşturur. Veritabanının dağıtık yapısı, DLT üzerinde gerçekleştirilen içerik ve işlemleri doğrulamak için karmaşık matematiksel algoritmaların kullanılmasını zorunlu kılar.

Geleneksel veri tabanlarından farklı olarak, DLT'ler, veri tabanında kaydedilen her değişikliği herkesin doğrulamasına izin veren bir kriptografik bilgi saklama sistemi uygular. Karmaşık matematiksel algoritmalar sayesinde bu birleştirme, zaman içinde her blokta yer alan bilgilerin değiştirilemeyeceğini garanti eder. Veritabanı çok fazla sayıda düğüm üzerine dağıtık olsa bile, defterin her bir kopyasının sağlam olduğu ve bu nedenle tüm düğümlere dağıtılan tüm bilgilerin birbiriyle uyumlu olduğu her zaman doğrulanabilir.

DLT'lerin bu özellikleri, merkezi bir otorite olmaksızın sistemin bütünlüğünü ve işleyişini sağlar. Ağı kendileri yöneten matematiksel modeller, sistemin doğru çalışmasını, tam bütünlüğünü ve değişmezliğini garanti eder. Dolayısıyla bu özelliklerin ışığında blokzinciri, özellikle kamu ve izinsiz olanlar olmak üzere, kamu idarelerinde şeffaflığının sağlanmasında önemli rol oynar.

3.2. Blokzinciri

Bu teknoloji bu kadar karmaşıksa, neden buna "Blockzinciri" diyoruz? En temel seviyesinde Blockzinciri, kelimenin tam anlamıyla sadece bir blokların zinciridir, ancak bu kelimeler geleneksel anlamında değildir. Bu bağlamda "blok" ve "zincir" kelimelerini söylediğimizde aslında halka açık bir veri tabanında (zincir) saklanan dijital bilgilerden (blok) bahsediyoruz.

Birçokları için "blokzinciri" terimi, genellikle geleneksel para birimleriyle ilişkilendirilen normların çoğuna meydan okuyarak önemli bir kamu ilgisi kazanan bir kripto para birimi olan Bitcoin ile eşanlamlı hale geldi. (Iansiti ve Lakhani, 2017)

Blokzinciri, Satoshi Nakamoto tarafından geliştirilen basitçe dağıtık bir defter teknolojisidir. 2008'in sonlarında, Satoshi Nakamoto adlı bir birey veya bir grup, güvenilir bir üçüncü tarafa ihtiyaç duymadan çalışmak üzere tasarlanmış, merkezi olmayan bir dijital ödeme sistemi olan Bitcoin'i tanıtan bir makale yayınladı (Nakamoto, 2008). Tanıtımı, internette ticaretin nasıl gerçekleştiğine bir cevaptı. Önceden, bir kişi bir ödeme yapmak istediğinde veya para birimini dijital olarak transfer etmek istediğinde, bu işlemi gerçekleştirmek için güvenilir bir üçüncü tarafa (örneğin bir banka) ihtiyaç duyuluyordu. Bitcoin'de, iki taraf bu türden güvenilir üçüncü şahıslara ihtiyaç duymadan işlem yapabilecektir (Nakamoto, 2008).

Nakamoto'nun orijinal makalesinde blokzinciri teriminden hiç bahsedilmedi. Bununla birlikte, Bitcoin'in birbirine zincirlenmiş bir dizi zaman damgalı veri bloğunu kullanma şekli, günümüzde blokzinciri olarak bilinen olgunun kaynağı olarak algılanmaktadır (Mattila, 2016).

Santoshi'nin gördüğü sorun, tüm işlemlerin mevcut tüm ödeme sistemlerinde büyük ölçüde güvene bağlı olmasıdır. Birincisi, mevcut elektronik ödeme sisteminde, tüm işlemler yetkili bir kişi üzerinden geçer, kural olarak banka böyle bir kişi gibi davranır. Bir aracıya atıfta bulunmak, her operasyonu daha pahalı hale; bu çerçevede sık veya

küçük işlemleri kârsız hale getirir, ancak Nakamoto'nun eşler arası elektronik işlemlerinin bulguları ile merkezi güven yerine kriptografik kanıta sahip olunması, çevrimiçi ödemelere izin vererek üçüncü tarafların katılımına ihtiyaç duymadan doğrudan aktarılabilir. (Nakamoto, 2008.)

Nakamoto'nun makalesi sunulduktan sonra, blokzinciri teknolojisinin rolünü açıklayan çok sayıda yayınlanmış çalışma ve araştırma ortaya çıktı. Drescher (2017, 35), blokzincirini merkezi olmayan, dağıtık eşler arası kayıt sistemi ve ortak uygulama alanı olarak tanımlamaktadır. Bilgi içeriği sıralanır ve belirli düzenlemeleri izleyen her bir yapılandırılmış veri bloğu arasına bağlanır. Kriptografi kanıtı ve karma algoritma ile birleştirilmiş güvenlik teknolojileri, herhangi bir dahili veya harici değişikliğin gerçekleştirilmesine izin vermeyerek, bütünlüğü elde etmek ve korumak için kullanılmaktadır. Blokzincirin tanımı belirsizdir, teknolojik, ticari veya yasal gibi farklı durumlar için uygulanabilir. Blokzincirleri, güvene dayalı bir alan, bir değişim ortamı, güvenli bir kanal, bir dizi merkezi olmayan yetenek ve hatta daha fazlası olarak düşünülebilir. (Mougayar, 2016, s. 23)

Blokzinciri, işlem verilerini barındıran, sürekli büyüyen bir blokzinciri olan dağıtık defterdir. Bu bloklar kriptografik olarak güvenlidir ve zaman damgalarına sahiptir, sonuç olarak her blok bir öncekine bağlıdır (Martindale, 2018). Blozinciri, düğümler (blokzincirinin katılımcıları) arasında dağıtılır ve yeni bir blok doğrulandığında, hemen tüm düğümlere eklenir. Özünde, blokzincirinin amacı, taraflar arasındaki işlemler sırasında güven sorununu çözmektir. Bir dizi işlem, blokzincirine eklenecek yeni bir blokta bir araya getirilir. Hiçbir düğüm blokzincirini yeniden yazamaz veya hileli işlemleri doğrulayamaz ve tek bir düğüm yok edilirse ağ hala çalışır durumdadır.

Kavramsal düzeyde, blokzinciri, iki tarafın üçüncü taraf bir otoriteye ihtiyaç duymadan birbirleriyle yasal olarak işlem yapmasına izin verir. Geleneksel olarak, meşru bir işlem, işlemi yöneten ve her iki tarafın da işlemin sonucunu desteklediğinden emin olan bir aracı gerektirir. Anonimlik ve ademi merkeziyetçilik yönleri, blokzinciri ve interneti oldukça benzer kılmaktadır. Blokzinciri, teknolojik yenilik bağlamında genellikle internetle karşılaştırılır (Iansiti ve Lakhani, 2017), ancak aralarında önemli bir fark vardır. İnternet temelde teknolojik bir yenilikken, blokzincirinin internet gibi temelde yenilik olduğu tartışılabilir (Davidson, Filippi, ve Potts, 2016, s.15). Blokzinciri elektronları daha hızlı hareket ettirmez, ancak kriptografik

mekanizmalarla ihlalleri ortadan kaldırarak işlem maliyetlerini düşürür (Davidson ve diğerleri, a.g.m.). Bu açıdan blokzinciri, yeni yönetişim biçimleri için temel bir teknolojidir (Davidson ve diğerleri, 2015, s. 3). Başka bir deyişle, blokzincirler, insanların ekonomik eylemlerini koordine etmek için kurumsal alternatifler olarak piyasalarda kuruluşlarla rekabet eder (Davidson ve diğerleri, a.g.m.).

3.3. Blokzincirinin Temel Özellikleri

Yukarıdaki genel bakışa dayanarak, blokzinciri sistemini mevcut defter ve veritabanı teknolojisinden ayıran temel özellikleri şu şekilde özetlenebilir: Blokzinciri sistemleri *dağıtık, şeffaf, güveni sağlayan ve değişmez*dir. Buna göre, gelişmiş veri güvenliği, ağ esnekliği ve verimliliği sağlar.

3.3.1. Dağıtık Yapı

Bir blokzinciri sisteminde, veritabanı, bir sunucuda merkezi olarak konumlandırılmak veya merkezi bir otorite tarafından tutulmak yerine, ağda dağıtılan tüm düğümler tarafından tutulur ve tutulur. Defterde yapılan herhangi bir değişiklik, tüm düğümler tarafından kabul edilir. Konsensüs kurulduğunda, her düğüm kendi defterini güncelleyecektir (OECD, 2018). Bu dağıtık yapı, merkezi ve yoğun bir otoritenin sağladığı bir güvenilirlik düzeyi sağlar.

3.3.2. Konsensüs Yoluyla Şeffaflık ve Güven

Blokzinciri sistemleri birbirlerine tam olarak güvenmeyen veya işlemleri doğrulamak veya anlaşmazlıkları çözmek için herhangi bir merkezi otoriteye güvenmeyen taraflar arasında doğrudan, eşler arası işlemleri mümkün kılmak için tasarlanmıştır. Taraflar birbirlerine güvenmeseler bile, bilgileri değiştirmeye karşı korumalı bir şekilde kaydedecek teknolojiye güvenebilirler. Bu, sistemi şeffaf hale getirir ve sonuç olarak güven oluşur. Blokzinciri, böyle bir güven oluşturmak için bir fikir birliği mekanizmasını kullanır. Konsensüs protokolleri, tüm düğümlerin izlemeyi kabul ettiği bir dizi kural formüle eder ve ağ boyunca yayılan her düğümün aynı yeni bloğu eklemesini sağlar (OECD, 2018). Çünkü bu protokoller kodla uygulanır ve tek bir düğümün çıktısıyla karşılaştırılarak kolayca test edilebilir.

3.3.3. Değişmezlik

Geleneksel bir veritabanı sisteminde, yetkili bir kullanıcı genellikle veritabanında depolanan verilere erişebilir, bunları değiştirebilir ve hatta kalıcı olarak silebilir. Öte yandan, blokzincirindeki veriler değişmezdir. Veriler blokzincirine birleştirildikten ve kaydedildikten sonra, geri dönüp bloğun içeriğini değiştirmek son derece zordur (Bashir, 2017). Ayrıca, blokzincirinde bulunan veriler binlerce bağımsız düğümde depolandığından, herhangi bir düğümün değiştirilmesi genel fikir birliğini etkilemeyecektir (OECD, 2018).

3.4. Blokzinciri Sınıflandırması

Blokzinciri, gerçekleştirdiği işlem türüne ve düğümlere göre genel olarak üçe ayrılır.

3.4.1. Özel (İzin Verilen) Blokzinciri

İzinli bir Blokzinciri, işletme içindeki etkileşimin, ağ sahibi/sahipleri tarafından sağlanan erişim haklarına sahip kullanıcılarla sınırlı olduğu bir blokzinciridir ve kurumsal blokzinciri olarak da bilinir. Böyle bir ağda, blokların anonim olmayan doğrulanmasına veya blokzinciri ile etkileşimine izin verilmez. Genellikle, böyle bir ağa erişimi yönetmek için bir sertifika setkilisi kullanılır**.** Ağını izinli bir ağ olarak çalıştıran bir blokzinciri platformu, kimin doğrulayıcı olabileceğini ve hangi kullanıcılara hangi ayrıcalıkların verildiğini belirleyecektir. Hyperledger Fabric, izin verilen bir blokzinciri çerçevesinin en belirgin örneklerinden biridir. Öte yandan, özel izinsiz blokzinciri doğrulamaya açık, ancak okumaya kapalı olmalıdır (Rikken, Janssen ve Kwee, 2019).

3.4.2. Açık Blokzinciri (İzinsiz)

Herkese açık bir blokzinciri, herkes tarafından (genellikle anonim olarak) erişilebilen bir blokzinciridir. İşlemler matematiksel olarak geçerliyse, kimlerin katılabileceği ve hangi işlemleri yayınlayabileceği konusunda herhangi bir kısıtlama yoktur. Üyeler ağa isimsiz olarak katılabilseler de (yalnızca açık anahtarlarını ifşa ederek), üstlendikleri her işlem herkes tarafından görülebilir (genel), bu da kullanıcıları belirlemek için dikkatlice incelenebilir. Bitcoin, halka açık blokzincirinin en ünlü örneğidir. Böyle bir

ağda, tipik olarak, katılımcılara yoğun bir bilgi işlem kaynağı konsensüs protokolünü yürütmeleri için verilen bir teşvik vardır.

3.4.3. Konsorsiyum Blok Zinciri

Konsorsiyum blokzinciri modeli, Özel Blokzincirine çok benzer. Konsorsiyum blokzincirini farklı kılan şey, özel blokzincirinde kontrol edilen tek bir tarafın, konsorsiyum blokzincirinde kontrol edilen birden fazla tarafın olmasıdır. Tek bir kuruluşun blokzinciri (merkezileştirilmiş) sürdürmesi ve etkileşimde bulunan taraflara önceden tanımlanmış erişim hakları sağlaması mümkündür. Böyle bir ağ, tipik olarak diğer katılımcılar üzerinde yasal yetkisi olan hükümet veya düzenleyici kurumlara uygundur. Bununla birlikte, defterler merkezi olarak depolandığından ve katılan düğümler arasında dağıtılmadığından, böyle bir ağa blokzinciri ağı denilip adlandırılmayacağı tartışmalıdır. Ana hedef, daha merkezi olmayan bir özel blokzincirine ulaşmaktır.

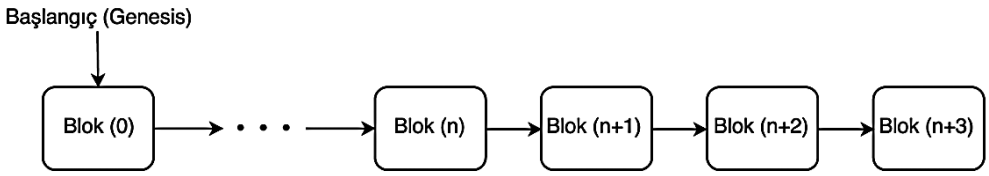
3.5. Blokzinciri Altyapısı

Blokzincirinin bütün bir sistem olarak çalışma prensibini anlamak için, içerdiği ana unsurları belirlemek gerekir. Genel olarak, blokzincirinin mimarisi veri katmanı, ağ katmanı, fikir birliği katmanı, teşvik katmanı ve uygulama katmanı olmak üzere beş katman olarak organize edilebilir (Shen, Zhu ve Xu, 2021, s. 16).

3.5.1. Veri Katmanı

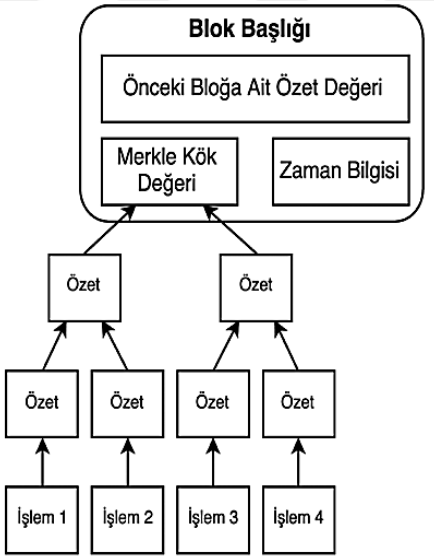
Veri katmanı, blokzincirinin veri yapısını ve bu tür bir yapıyı oluşturmak için kullanılan ilgili teknikleri içerir.

Zincirli yapı: Blok, blokzincirinin temel bileşenleridir. Her bir blok, bir dönem boyunca üretilen işlemleri kaydeder. Defter verilerinin değişmezliğini sağlamak için, her blok önceki bloğun karmasını kendi blok başlığında kaydeder ve ardından mevcut bloğun karmasını hesaplar. Böylece, bloklar, Şekil 3.1.'de gösterildiği gibi kronolojik sırayla doğrusal olarak bağlanır. Her bloğu ana bloğuna bağlayan hash dizisi, şimdiye kadar oluşturulan ve genesis bloğu olarak bilinen ilk bloğa kadar uzanan bir zincir oluşturur. (Antonopoulos 2017, 535.)



Şekil 3.1. Blokzincirin zincir yapısı

Veri blokları: Bir blok, blok başlığı ve blok gövdesinden oluşur. Blok başlığı blok sürümü, merkle kök değeri, zaman damgası, nBits, nonce ve önceki blok değeri alanlarını içerir. Blok sürüm, izlenecek doğrulama kuralları düğümlerini belirtir. Merkle kök değeri bloktaki tüm işlemlerde hesaplanır. Zaman damgası 1 Ocak 1970'den beri geçerli zamanı kaydeder. NBits, bir blok karmasının doğrulanmasını gösterir. Nonce, bir bloğu doğrulamak için madenci tarafından ayarlanır. Önceki blok değeri, önceki bloğa işaret eden 256 bitlik bir hash değeridir.



Şekil 3.2. Dört işlemli bir merkle ağacı örneği

Merkle Ağacı: Merkle ağacı, her bir işlemin başka bir işlemle eşleştirilmesi ve bunlara sağlama uygulanmasıyla oluşturulur. Hesaplanan sağlamalar ayrıca bir başka sağlamalarla ile eşleştirilir ve tekrar sağlama yapılır. Bu tür bir süreç, yalnızca bir merkle kökü kalana kadar tekrar eder. Şekil 3.2.'de, bir merkle ağacının nasıl inşa edildiğine dair bir örnek gösterilmektedir.

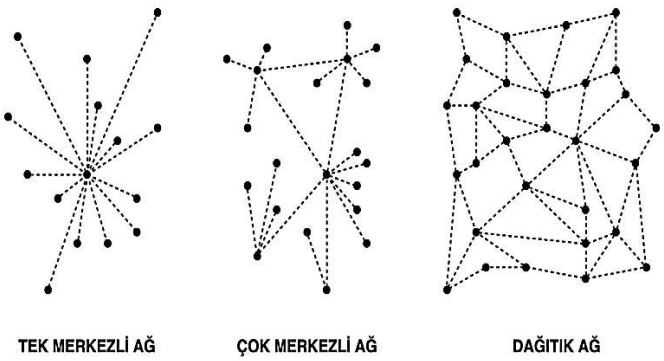
Özet fonksiyonu: Özet işlevi, merkle kökünün özetini yinelemeli olarak hesaplamak için kullanılır. Ayrıca her bir blok özet değeri sonraki blokta saklanır. Bu şekilde, veriler yazıldıktan sonra defteri değiştirmek neredeyse imkansızdır. Bitcoin'de SHA-256 algoritması kullanılmaktadır.

İşlemler: İki tür işlem vardır: madeni bazlı işlemler ve ortak işlemler. Madeni işlemler madenciler tarafından oluşturulur. Ortak işlemler, işlem teklifi gönderen herkes tarafından oluşturulabilir. Ortak işlemler, iş uygulamalarından üretilen verileri içerir.

Asimetrik kriptografi: Blokzinciri sistemlerinde, imza mekanizması esas olarak kullanılan asimetrik kriptografidir. Bitcoin adresi, bir imza anahtar çiftinin genel anahtarından türetilir. Her işlem, kaynağını kanıtlamak için kendi özel imza anahtarını kullanarak gönderen tarafından imzalanır.

3.5.2. Ağ Katmanı

Blokzincirinde herhangi bir merkez bulunmamaktadır. Algoritma, blokzincirinin işlendiği bütün bilgisayarlarda eşlenik olarak bulunur. Bu durum dağıtık yapı olarak adlandırılır. Bu bilgisayarların her birine "node" yani düğüm ismi verilmiştir. Ağ katmanı, blokzinciri ağında kullanılan protokolleri, yani blokzinciri ağını oluşturmak için kullanılan Eşler Arası (P2P) protokolü, işlem önerilerini ve yeni yürütülen işlemleri yayınlamak için kullanılan yayılma protokolünü ve doğrulamak için kullanılan doğrulama protokolünü içerir.



Şekil 3.3. Ağların karşılaştırılması (Baran, 1964)

P2P protokolü: Tüm blokzinciri ağ düğümleri belirli P2P protokolü kullanılarak düzenlenir. Bir P2P ağındaki düğümler eşit güce sahiptir ve aynı görevleri yerine

getirir. Genellikle, her bir düğüm dosyaların bir kopyasını tuttuğu için merkezi bir yöneticileri yoktur- bireysel bir eş gibi davranır. Bir P2P protokolü, düğümlerin nasıl organize edileceğini belirler. P2P protokolü, bir düğümün keşfettiği ve ilk başladığında diğer eşlerle bağlantı kurduğu mekanizmayı açıklar. Protokol, bir düğümün, bağlı eşler çevrimdışı olduğunda bağlantılarını yeni eşlerle güncelleme stratejisini açıklar. Ayrıca protokol, bir düğümün yerel verilerini diğer eşlerden senkronize ettiği mekanizmayı açıklar.

Yayılma protokolü: Yayılma protokolü, genellikle veri senkronizasyon görevini gerçekleştiren P2P protokolünün bir alt parçası olarak hareket eder. Blokzinciri sistemlerinde, işlem tekliflerinin, yürütülen işlemlerin veya blokların, bir düğüm bu tür verileri başlattığında veya aldığında başkalarına yayınlanması gerekir. Bitcoin'de, bir madenci yeni bir blok keşfettiğinde, yeni bloğu belirli yöntemlerle emsallerine yayınlar.

Doğrulama protokolü: Benzer şekilde, doğrulama protokolünün, işlemlerin yapılandırıldığı kuralları ve bir blok halinde nasıl organize edildiklerini tanımlayan özellikler olması daha olasıdır. Örneğin, Bitcoin'de bir madenci, giriş adreslerinin bitcoininin harcanmadığını doğrular. Eşler, yerel blokzincirlerine eklemeden önce işlemi ve yeni eklenen bloğun özet değerini yeniden doğrular.

3.5.3. Mutabakat Katmanı

Blokzinciri, dağıtık bir defterdir. Geleneksel merkezi defter sistemlerinden farklı olarak, yürütülen işlemleri doğrulamak için herhangi bir merkezi otorite mevcut değildir. Bununla birlikte, blokzinciri, kullanıcılarına tutarlı defter verileri sağlamak zorundadır ve mutabakat burada devreye girer. Mutabakat, herhangi bir blokzinciri ağının temel parçasıdır. Mutabakat, bir blokzinciri ağındaki tüm düğümlerin dağıtık ağın mevcut durumu hakkında merkezi otorite olmadan ortak bir anlaşmaya varmasını sağlayan bir prosedürdür. Bu şekilde, blokzinciri ağı, dağıtık bir ortamda bilinmeyen eşler arasında güvenilirlik sağlar ve güven oluşturur. Esasen, mutabakat, her bir eşe eklenen her yeni bloğun tutarlı olmasını garanti eder ve bu blokzinciri ağındaki tüm eşler tarafından kabul edilir. Mutabakat protokolleri olarak başlıca Proof of Work (POW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Pratik Bizans Hata Toleransı (PBFT) gibi tipik fikir birliği algoritmaları bulunmaktadır.

Emeğin Ispatı (Proof of Work-PoW): PoW, Bitcoin'de kullanılan fikir birliği algoritmasıdır. Ağın her düğümü, blok başlığındaki özet değerini hesaplar. Blok başlığında rastgele bir sayı (Nonce) vardır, böylece madenciler farklı özet değerleri elde etmek için değişebilir. Fikir birliği, hesaplanan özet değerinin nBits alanında ayarlanan eşikle karşılanmasını gerektirir. Bir madenci böyle bir özet değeri elde ettiğinde, yeni bir blok oluşturma ve bloğu başkalarına yayınlama hakkına sahiptir. Diğer tüm düğümler, karma değerin doğruluğunu onaylar. Bu şekilde yeni blok, ana blokzincirine diğer düğümler tarafından eklenerek doğrulanır.

Sahipliğin Ispatı (Proof of Stake-PoS): PoS bilgi işlem kaynaklarından büyük ölçüde tasarruf sağlayabildiğinden, enerji tasarrufu için PoW'a bir alternatiftir. Madenciler, token miktarına sahip olduklarını kanıtlamalıdırlar. Daha fazla token sahibi olduğu sürece bir kullanıcının madenci olarak seçilme olasılığı daha yüksektir. PoW ile karşılaştırıldığında, PoS önemli ölçüde enerji tasarrufu sağlar ve daha verimlidir. Bu nedenle, başlangıçta PoW'yi benimseyen birçok blokzinciri, kademeli olarak PoS'ye geçmeyi planlamaktadır. Örneğin, Ethereum Ethrash'tan (PoW'un bir çeşidi) Casper'a (PoS'nin bir çeşidi) dönüşmeye çalışmaktadır.

Yetkilendirilmiş Sahipliğin Ispatı (Delegated Proof of Stake-DPoS): DPoS tüm ademi merkeziyet özelliğini feda etme pahasına yüksek ölçeklenebilirlik sağlayabilen bir PoS çeşididir. DPoS'da, blokları bir sıralı sırayla üretmek için yalnızca belirli sayıda seçilmiş düğüm (blok üreticileri veya tanıklar olarak adlandırılır) seçilir. Bu blok üreticileri, sahip oldukları token sayısı, yani hisseleriyle orantılı olarak bir dizi oy alabilen tüm ağ katılımcıları tarafından seçilir. Alternatif olarak, kullanıcılar oylarını başka bir seçmene devretmeyi seçebilir ve bu seçmen de hedef blok üreticilerini kendi adına oylayabilir. Bir DPoS ağındaki blok üreticilerinin sayısı, o zincirin somut kurallarına bağlıdır. Kötü niyetli olduğu tespit edilirse, bir blok üreticisinin gücü kesmesi mümkündür. Böyle bir durumda seçmenler bir sonraki turda kendilerine oy vermeyebilir. DPoS, blok üreticisinin sayısını önemli ölçüde sınırlayarak, yüksek ölçeklenebilirlik kazanır ve birden çok büyüklükteki işlem hacmini idare edebilir.

Pratik Bizans Hata Toleransı (Practical Byzantine Fault Tolerance-PBFT): PBFT, 1999 yılında Barbara Liskov ve Miguel Castro tarafından sunulan ve Bizans hatalarını tolere eden asenkron sistemlerde verimli bir şekilde çalışmak üzere tasarlanmış bir çoğaltma algoritmasıdır. Bir PBFT sistemi, maksimum kötü amaçlı düğüm sayısının

sistemdeki tüm düğümlerin 1/3'ünden daha az veya buna eşit olması koşuluyla iyi bir şekilde çalışabilir. PBFT 3 aşamaya ayrılmış turlar halinde çalışır: istek, önceden hazırlanmış, hazırlanmış ve taahhütlü. PBFT sistemlerinde, yalnızca bir düğüm birincil düğümdür ve diğerleri ikincil düğümler olarak adlandırılır. Her turda, bazı kurallara göre bir birincil düğüm seçilir. Birincil düğüm bir istemciden bir istek aldığında, birincil düğüm, isteği ikincil düğüme yayınlar. Düğümler (hem birincil hem de ikincil) istenen hizmeti gerçekleştirir ve ardından istemciye bir yanıt gönderir. İstek başarıyla yerine getirilir, yalnızca müşteri aynı sonucu veren m + 1 yanıt alır; burada m, izin verilen maksimum hatalı düğüm sayısıdır.

3.5.4. Teşvik Katmanı

Token, en yaygın olarak blokzinciri sistemlerinde teşvik mekanizmalarını uygulamak için kullanılır, örneğin Bitcoin sisteminde BTC, Ethereum sisteminde ETH vb. tokenlerin genellikle parasal değeri vardır ve bunlar yasal para birimiyle takas edilebilir.

Tokenlerin verilmesi ve dağıtılması teşvik mekanizmalarının ana parçalarıdır. Token verme mekanizması, jetonun nasıl üretileceğini belirler, bu da toplam token miktarını artırır. Token dağıtım mekanizması, mevcut tokenlerin farklı kullanıcılar arasında nasıl dağıtılacağını belirler.

Bitcoin sisteminde, var olabilecek toplam bitcoin miktarı 21 milyondur. Şu anda, her yeni blok oluştuğunda, madenciye dolaşım için 12,5 bitcoin verilmektedir. Bu tür madencilik ödülleri, her 210.000 blok üretildiğinde azaltılır.

3.5.5. Uygulama Katmanı

Geliştiriciler, yalnızca ek veritabanı olarak temeldeki blokzincirini kullanarak iş uygulamalarını geliştirebilirler. Bu tür bir iş mantığı, blokzinciri sistemleri tarafından sağlanan programlama mekanizması kullanılarak uygulanır; örneğin, komut dosyası, akıllı sözleşme, zincir kodu, vb.

Script: Script, Bitcoin için bir kilitleme mekanizması olarak kullanılan, Bitcoin'de sağlanan bir mini programlama dilidir. Her çıktıya bir kilitleme betiği yerleştirilir. Buna karşılık olarak, bir giriş olarak kullanıldığında bir çıktının kilidini açmak için

işlemde bir kilit açma komut dosyası sağlanmalıdır. Bir betik iki bölümden oluşur: veri ve operasyon kodları. Operasyon kondları, veriler üzerinde çalışan basit işlevlerdir.

Akıllı Sözleşme: Ethereum Sanal Makinesi (Ethereum Sanal Machine-EVM) üzerinde çalışan programlar genellikle akıllı sözleşmeler olarak adlandırılır. Solidity, yazmak için en popüler dildir. Akıllı Sözleşmeler, ilişkili tarafların kapsam üzerinde anlaşmalarından sonra hazırlanıp, kriptografik olarak imzalanıp, blokzinciri ağına yüklenirler. Yüklenmiş sözleşmeler, blokzinciri ağı üzerinde olan diğer bileşenlerle etkileşim kurabilirler. Bu etkileşim bir işlemin başlatılması olabileceği gibi bir bilginin gönderilmesi/teslim alınması şeklinde olabilir. Sözleşme hazırlanırken belirlenmiş durumlar oluştuğunda, akıllı sözleşmeler otomatik olarak içerisinde tanımlanmış olan anlaşma koşullarının çalıştırılmasını sağlar. (Usta ve Doğantekin, 2019, s.133)

Yürütülebilir kodlar, bir anlaşmanın şartlarını yerine getirmeyi ve tarafları uymaya zorlamayı kolaylaştırır (Alharby ve Van Moorsel, 2017). Akıllı sözleşmeler, herhangi bir zamanda karar verilen durumlarda uygulanan bir dizi kural olarak düşünülebilir. Yeni bir teknoloji değillerdir ama blokzinciri teknolojisi onları görünür kılmaktadır (Alharby ve Van Moorsel, 2017). Günümüzde birçok uygulama (özellikle merkezi olmayan uygulamalar) akıllı sözleşme teknolojisini kullanmakta, böylece üçüncü şahıslara duyulan ihtiyaç azaltılmakta veya ortadan kaldırılmaktadır (Rikken ver diğerleri, 2019).

Zincir Kodu (Chaincode): Zincir Kodu, akıllı sözleşmeye benzer şekilde çalışır. Hyperledger Fabric'te bir terminolojidir. Chaincode, Go, node.js veya Java'da yazılmış ve önceden belirlenmiş bir arabirimi uygulayan bir programdır. Blokzinciri defteri, zincir kodları tarafından başlatılır ve yönetilir. Uygulamaların defter durumunu değiştirmek için zincir kodlarını çağırması gerekir.

Merkezsiz Uygulama (Decentralised Application-dApp): dApp, resmi veya üçüncü bir tarafça sağlanan Yazılım Geliştirme Kiti (Software Development Kit-SDK) tarafından çağrılan komut dosyasını, akıllı sözleşmeyi veya zincir kodunu içeren türden uygulamalardır. Genellikle sıradan kullanıcılara kullanıcı dostu arayüzler sağlayabilirler. Ethereum'da oyun ve değişim en popüler iki dApp'dir. Blokzinciri imalat, sağlık hizmetleri, küçük işletme, tedarik zinciri, dijital kimlik, perakendeciler vb. gibi giderek daha fazla sektöre uyarlamak üzere hyperledger olarak birçok çalışması bulunmaktadır.

3.6. Blokzinciri'nin Güçlü Yönleri

3.6.1. İşlemlerin Bütünlüğü

Dağıtık bir defter sistemi olarak, blokzinciri, yapılan her işlemi kaydeder ve doğrular, bu da onu güvenli ve güvenilir kılar. Veri paylaşımı senaryosunda, veri tüketicileri büyük ölçüde veri bütünlüğü olarak bilinen verilerin güvenilirliğine ve gerçekliğine bağlıdır. Veri bütünlüğü, verilerin tüm yaşam döngüsü boyunca sürdürülmesini ve doğruluğunun ve tutarlılığının güvence altına alınmasını içerir. Veri paylaşımı işlemi ve gerçek paylaşım verileri bir dereceye kadar parça işlemleri olarak kodlanabilir ve ayrıca blokzinciri tarafından kaydedilebilir (Zheng, Zhu, Shen ve diğerleri, 2018). Böyle bir durumda, veri tüketicisi, blokzinciri iyi veri bütünlüğü sağladığından, paylaşılan verilere yüksek oranda güvenebilir

3.6.2. Defterin Değişmezliği

Tasarım gereği, blokzinciri doğal olarak verilerin değiştirilmesine karşı korumalıdır. Blokzinciri defterinin değişmezliği, işlemlerin blokzincirine kaydedildikten sonra düzenlenemeyeceği veya silinemeyeceği anlamına gelir. Ek olarak, blokzincirleri aynı zamanda veriler için bir zaman tutma mekanizmasıdır, bu nedenle verilerin geçmişi kolayca raporlanabilir. Veriler bir blokzinciri sisteminde paylaşıldığı sürece, kaydedilen paylaşım verileri veri sahibi tarafından sağlanan orijinal veriler olduğu kabul edilir. Değişmezliğin özelliği nedeniyle, veri paylaşım işlemlerinin geçmişine atıfta bulunarak veri sağlayıcıların karlarını hesaplamak kolaydır.

3.6.3. Defter Mutakabatı

Blok zincir sistemlerinde, defteri kaydeden bir merkezi otorite veya üçüncü taraf yoktur. Bunun yerine, blokzinciri defteri bir dizi eş tarafından tutulur. Bu şekilde, bir kuruluşun, merkezi sistemlerin dezavantajlarından biri olan defter verilerini değiştirmesi veya taklit etmesi zordur. Daha iyi bakım için, veri sağlayıcıları ve tüketiciler, tüm ağ katılımcılarının uyması gereken kuralları müzakere edebilir. Öngörülen kuralları ihlal eden tüm işlemler reddedilir.

3.6.4. Kimlik Doğrulanabilirliği

Konsorsiyum sistemlerinde, blokzinciri defteri, bir konsorsiyumdan oluşan önceden seçilmiş birkaç düğüm tarafından tutulur. Ağa yalnızca yasal kullanıcılar katılabilir. Özellikle Hyperledger Fabric'te, ağ katılımcılarını kontrol etmek ve onlara uygun ayrıcalıkları yetkilendirmek için tasarlanmış bir üye mekanizması vardır. Ağ katılımcılarının denetlenmesi, veri paylaşım senaryosunda faydalı olabilir.

3.7. Blokzinciri'ne Yönelik Güvenlik ve Gizlilik Tehditleri

3.7.1. Blokzinciri'ne Saldırılar

Blokzinciri sistemlerinde çok sayıda saldırı vardır (Huynh, Nguyen ve Tan, 2019); örneğin % 51 saldırısı, tutulma saldırısı, bencil saldırı vb. Daha fazla bilgi işlem kaynağına sahip bir madenci, nonce değerini diğerlerinden daha hızlı bulmayı hesaplayacaktır, bu da % 51 saldırıya yol açabilir. Tutulma saldırısında, sahtekâr bir düğüm, kurbanları blokzinciri ağındaki diğer eşlere karşı kontrol altında tutmaya çalışır. Bencil madencilik saldırısı, dürüst olmayan bir madencinin halka açık zincirden daha fazla blok keşfetmek için yeterli bilgi işlem gücüne sahip olması durumunda gerçekleşir.

3.7.2. İşlem Verilerinin Gizlilik Sızıntısı

Blokzincirinde kaydedilen tüm işlemler açık metin olarak saklanır. Bir blokzinciri gezgini kullanarak, bir işlemin her alanında bulunan veriler başkaları tarafından kolayca öğrenilebilir. Blokzinciri defteri tüm eşlere açıktır, böylece her bir eş, defterde hangi verilerin depolandığını bilebilir. Bu şekilde, hassas veriler kamuya açıklanabilir (Malavolta, Moreno-Sanchez, Kate, Maffei ve Ravi, 2017). Bazı kullanıcılar yalnızca paylaşılan verilerinin herkes yerine yalnızca kısıtlı kullanıcılar tarafından görülebilmesini istediğinden, kullanıcıların veri paylaşmasını engelleyebilir.

3.7.3. Veri Temsiliyle İlgili Sınırlar

Blokzincirinde depolanacak tüm veriler, önceden belirlenmiş alanlar halinde biçimlendirilir. Bu şekilde düğümlerin işlemleri işlemesi uygundur. Ancak, farklı sektörlerdeki veriler tamamen farklıdır. Veri paylaşımı farklı sektörleri kapsayan

katılımcıları içerdiğinde, sektörlere jenerik olan esnek bir veri format depolama mekanizmasına ihtiyaç vardır. (Shen ve diğerleri, 2021)

3.7.4. Veri Depolama Sınırları

Bireysel blokzinciri defteri tipik olarak kilobayt düzenindedir ve yalnızca sınırlı veri tutulur. Bununla birlikte, blokzincirinin günlük yapısı, tüm işlem işlemlerinin blokzincirine kaydedildiğini ima eder. Kullanıcıların başkalarıyla veri paylaşırken bekledikleri de budur. Birçok veri işlemi, veriler veri tüketicileri tarafından dolaştırıldığında gerçekleşir. Bu nedenle, yalnızca veri paylaşımı için değil, aynı zamanda veri işleme için de büyük bir depolama alanına ihtiyaç vardır.

3.7.5. İşlem Mutabakatındaki Gecikme

Tek bir düğüm tarafından kontrol edilen merkezileştirme sistemlerinin aksine, blokzinciri sistemleri coğrafi olarak dağınık olan birçok düğüm tarafından korunur. İşlemlerin, iletişim kurulmadan önce çok sayıda düğüm tarafından doğrulanması gerekir. Dahası, olasılıksal mutabakat algoritması kullanan blokzinciri sistemleri, geri döndürülemez olduğundan emin olmak için taahhüt edilen işlemleri kapsayan bloktan sonra yeterli blok eklenmelidir. Bu, işlem tamamlama veriminin düşük olmasına yol açar. Bununla birlikte, bazı gerçek veri paylaşımı uygulamalarında, daha yüksek işlem hacmine ihtiyaç vardır.

Bu bölümde blokzincirinin yapısı incelenmiştir. Dijital devlet bağlamında blokzinciri kullanımı hakkında daha net bir vizyon ortaya koymak için hem diğer ülkelerin deneyimlerinin öğrenilmesi hem de kendi bulunduğu aşamanın tespit edilmesi önem taşır. Bir sonraki bölüm diğer ülkelerdeki blokzinciri strateji, politika ve uygulamaları ile Türkiye'nin mevcut durumu açıklamaktadır.

4. DİJİTAL DEVLET BAĞLAMINDA BLOKZİNCİRİ: STRATEJİ, POLİTİKA VE UYGULAMALAR

Blokzinciri ve onun altında yatan dağıtık defter teknolojisi finans alanında bir teknoloji olarak ortaya çıkmakla birlikte, dijital dönüşüm ve inovasyon açısından sahip olduğu özellikler ile birçok alanda uygulama potansiyeli bulmuştur. Blokzincirinin finans ve varlık yönetimi gibi alanlardaki kullanım örneği aracılığıyla potansiyel gösterdiği özel sektöre ek olarak, kamu sektörü uygulamalarına olan ilgi de devam etmektedir. Kamusal uygulanmasına ilişkin çalışmalar, devletin mahremiyet, güvenlik, yönetişim, şeffaflık ve hesap verebilirlik gibi kavramlar etrafında toplanmaktadır. Ülkeler, blokzinciri teknolojisi ile ilgili politikalarını şekillendirmeye ve dijital kimlik, kayıtlar, dijital para birimi, tedarik zinciri yönetimi, sağlık, eğitim gibi kamu hizmetlerine uygulanabilirliğini araştırmaya devam etmektedir.

Alanyazında çok sayıda çalışma olmakla birlikte, blokzincirinin kamu sektörü tarafından kullanılmasına ilişkin olarak; uygulama aşamasına geçilerek deneyimlerin tespit edilip analiz edildiği kapsamlı çalışmalara AB ve OECD tarafından hazırlanan belgelerde rastlanmaktadır (Allessie, Sobolewski ve Vaccar, 2019; Lindman v.d., 2020). Söz konusu projeler, uygulandığı ülke, uygulama alanı ve uygulama düzeyi Tablo 4.1.'de özetlenmiştir.

No	Proje Adı	Ülke	Uygulama Alanı	Uygulama Düzeyi
1	Exonum arzi tapu kaydı	Gürcistan	Tapu kaydı; mülkiyet işlemleri (Exonum (Bitcoin) tarafından tescil edilmiş ve zaman damgalı 1,5 milyon arazi tapusu. Kullanıcı sayısı şu anda bilinmiyor)	Ulusal
2	Blokcerts akademik kimlik bilgileri	Malta	Akademik sertifikalar doğrulama; kişisel belgelerin saklanması ve paylaşılması (Kullanıcı sayısı bilinmiyor)	Ulusal
3	Chromaway mülkiyet işlemleri	İsveç	Mülkiyet işlemleri; tapu devri (Pilot uygulama yapıldı ve proje askıya alındı)	Ulusal
4	uPort merkezi olmayan kimlik	İsviçre	İkamet kanıtı, e-oylama, bisiklet kiralama ve park etme ödemeleri için dijital kimlik	Yerel
5	Infrachain yönetişim çerçevesi	Lüksemburg	Blokzinciri yönetimi	Ulusal
6	Emeklilik altyapısı	Hollanda	Emeklilik sistemi yönetmek	Ulusal
7	Stadjerspas akıllı kuponları	Hollanda	Düşük gelirli sakinler için sosyal yardım yönetimi. (15.000'den fazla gerçek kullanıcısı var, ancak artık tam olarak blokzinciri üzerinde çalışmıyor)	Yerel
8	Uzaktan oylama	ABD	60’dan fazla seçimde uygulandı	Ulusal/ Yerel
9	İşsiz kayıtları	İsveç	Cüzdan yazılımını yükleyen yaklaşık 1 000 kullanıcı	Ulusal
10	Kamu alım süreci	Belçika	Tedarik bildirimlerinin yayınlanması ve tedarik süreci kontrolü. (Kullanımda, ancak kullanıcılar hakkında bilgi eksik)	Yerel
11	Kamu alım süreci	İspanya	Sınırlı testte: 24 halka açık ihale düzenlendi.	Yerel
13	Fatura takip sistemi	Çin	Guangdong Belediyesi 10 milyondan fazla blockchain faturası kaydetti ve 7.000'den fazla şirket blokzinciri faturalandırma sistemine erişebildi (Kullanıcılar hakkında bilgi eksik).	Yerel
14	Şirket kayıt bilgileri	Kanada	1.3 milyon aktif tüzel kişilik, 2.4 milyon doğrulanabilir kimlik bilgisi (Kullanıcılar hakkında bilgi eksik)	Yerel/ Bölgesel

Tablo 4.1. Kamu sektörü blokzinciri uygulamaları
(Allessie, Sobolewski ve Vaccar, 2019; Lindman v.d., 2020)

Tablo 4.1.'de görüldüğü gibi ülkelerin dijital devlet bağlamında etkileşim ve birlikte çalışabilirlik maksatlı çalışma ve uygulamalarının çok sınırlı sayıda olduğu görülmektedir. Bu maksatla bu bölümde literatürde blokzinciri teknolojisine strateji ve politikalarında yer veren ve uygulayan başlıca ülkeler, kullanım örnekleriyle birlikte incelenmektedir. Ayrıca alanyazında yer alan, blokzinciri veri paylaşım çalışmalarına da yer verilmiştir. Son olarak Türkiye'deki blokzinciri çalışmaları ele alınmıştır.

4.1. Avrupa Birliği (AB)

Avrupa Komisyonu, politika, hukuk ve finansman alanlarında blokzincirini güçlü bir şekilde desteklemektedir (Avrupa Komisyonu, t.y.). Dijital devlet girişimlerinden fiili olarak uygulamaya konulanlardan ilki, 2018 yılında tüm AB Üye Devletleri, Norveç ve Lihtenştayn arasında bir işbirliği mekanizması kuran Avrupa Blokzinciri Ortaklığı'dır (European Blockchain Partnership-EBP) (Avrupa Komisyonu, 2018). Bu ortaklık, kurumlar arasındaki güveni ve verimliliği artırarak vatandaşların, kurumların ve işletmelerin etkileşim biçimini geliştirmek için blokzincirinin potansiyelinden yararlanmak ve yeni iş fırsatları yaratmaya ve oluşturmaya yardımcı olmak amacıyla ortak bir kamu sektörü girişimidir. İkincisi, GDPR (Genel Veri Koruma Yönetmeliği) ve eIDAS (Elektronik Kimlik Belirleme, Doğrulama ve İmza) gibi ilgili düzenlemelere uygun olarak, güvenlik, gizlilik veya sürdürülebilirlik açısından en yüksek standartlarla AB çapında kamu hizmetlerini veya kamu yararı alanlarındaki hizmetleri desteklemeyi amaçlayan Avrupa Blok Zinciri Hizmetleri Altyapısıdır (European Blockchain Services Infrastructure-EBSI) (Avrupa Komisyonu, 2020).

EBSI, Avrupa Komisyonu ve üye devletlerin (toplu olarak Avrupa Blok Zinciri Ortaklığı olarak faaliyet gösteren) ortak bir girişimidir. Girişimin belirtilen amacı, blokzincir teknolojisini kullanarak AB çapında sınır ötesi kamu hizmetleri sunmaktır. EBSI, gizlilik, siber güvenlik, birlikte çalışabilirlik ve enerji verimliliği açısından AB yasalarıyla tamamen uyumludur. (EBSI, t.y.)

EBSI, belirli kullanım durumlarına odaklanan uygulamalarla dağıtılmış düğümlerden oluşan bir ağ halinde düzenlenmiştir. İlk olarak 2019'da dört kullanım senaryosu seçilmiş ve her bir vakayı ele almak için farklı prototipler oluşturulmuştur. Seçilen

dört blokzinciri kullanım durumu noter tasdik, diplomalar, egemen kimlik ve veri paylaşımıdır.

Gerekli uygulama yazılımı, teknik özellikler ve mevcut servis desteği dahil olmak üzere farklı kullanım durumları hakkında çok sayıda materyal mevcuttur. Ek kullanım durumları eklenmeye devam edilmekte ve halihazırda mevcut uygulamalar kullanıma sunulmaktadır.

4.2. Estonya

Estonya blokzinciri teknolojisini kamusal alanda kullanan ilk ülkelerden biridir. Estonya, blokzincirini kurumların veri ve sistemlerinin bütünlüğünü sağlamak için kullanmaya başlamıştır (Priit Martinson, 2018). Estonya'nın blokzinciri altyapısını kullanım amaçları, kamu verilerine güven sağlamak, devlet verilerinin kötüye kullanılması durumunda tehditleri en aza indirmek ve devlete ait verilerin veritabanlarından bağımsız olarak gerçek zamanlı olarak doğrulanmasını sağlamaktır. (Özaltın ve Ersoy, 2020). Bu nedenle Estonya devlet kurumları geliştirdikleri blokzinciri tabanlı uygulamaların kontrolünü elinde tutarak, veritabanı entegrasyonlarını kendileri koordine etmektedir. Anahtarsız İmza Altyapısı (Keyless Signature Infrastructure-KSI) ve e-İkamet, blokzincir tabanlı inovasyonların önemli iki örneğidir.

Anahtarsız İmza Altyapısı (KSI), büyük ölçekli bilgileri kaydeden ve doğrulama sağlayan bir blokzinciri sistemidir (e-Estonya, t.y.). KSI'nin ana avantajı, veri bütünlüğü sağlamasıdır. Ek olarak, proje hükümet verilerine olan güven ve şeffaflığı arttırmıştır. KSI projesi Estonya Bilgi Sistemleri Kurumu koordinesinde oluşturulan, kamu kurum ve kuruluşlarının SDK ve önceden oluşturulmuş araçları kullanarak blokzinciri destekli teknolojinin uygulanmasından sorumlu olduğu bir yapıya sahiptir. Estonya hükümetinin bu alanda birkaç farklı kullanım durumu vardır. Bazı kullanım durumları için KSI blokzinciri, arşivleme ve sürüm oluşturmayı garanti etmenin yalnızca bir parçasıdır. Diğer kullanım durumları için, veri bütünlüğünün ana ve tek garantisidir. KSI projesinde iki teknik fayda vardır: blokzinciri tarafından desteklenen değişmezlik ve veriler üzerinde fikir birliği süreci. Projenin blokzincirinde veri depolanmayan blokzinciri destekli bir hizmet olduğu belirtilmektedir. Blokzinciri ağı, depolama için değil, yalnızca verilerin ve günlük değişikliklerinin bütünlüğünü garanti

etmek için kullanılır. KSI blokzinciri, halihazırda sağlık, mülk, işletme, miras sicili ile dijital mahkeme sistemini vb. korumaktadır (E-Estonya, t.y.). Bu çerçevede Adalet Bakanlığı, Ekonomik İşler ve Haberleşme Bakanlığı, Maliye Bakanlığı, İçişleri Bakanlığı ve Sosyal İşler Bakanlığı tarafından KSI kullanmaktadır.

Aralık 2014'te Estonya, blockzinciri girişimi olan Bitnation ile ortaklaşa, ülke içinde ve dışında bulunan kişilere elektronik ikamet olanağı sunan e-İkamet adlı bir çözümü, bu konuda dünyada ilk geliştiren ülke olmuştur. Proje, özel bir çip içeren bir kimlik kartı ile, belgeleri imzalamak ve dosya şifrelemek için dijital imza imkanı sunarak, başvuru sahiplerine Estonya'nın özel ve kamu kuruluşları tarafından sunulan hizmetlerden yararlanmasını sağlamaktadır (Alender, 2016).

Estonya e-İkamet kartı, kişisel kimlik belgesi yerine geçmemektedir, seyahat belgesi de değildir. Yine de belgelerin dijital olarak imzalanmasına, imzalanmış belgelerin gerçekliğinin doğrulanmasına, belgelerin güvenli bir şekilde şifrelenmesine ve iletilmesine, çevrimiçi bir Estonya şirketi kurulmasına, şirketin dünyanın her yerinden yönetilmesine, e-bankacılık ve uzaktan para transferleri yapılmasına, çevrimiçi ödeme hizmetine erişilmesine ve vergilerin çevrimiçi olarak beyan edilmesine olanak tanır. (e-Estonya, 2016)

4.3. ABD

Amerika Birleşik Devletleri'nde, blokzinciri konusunda birkaç farklı politika gözlemlenebilir. Federal hükümet, eyalet hükümetlerinin kendi politikalarını ve düzenlemelerini oluşturmasına ve uygulamasına olanak tanıyan bir yaklaşım benimsemiştir. İnovasyonu teşvik etmek için bazı eyaletler, blokzinciri dostu mevzuat geliştirerek blokzincirinin benimsenmesinin önündeki yasal engelleri kaldırma yaklaşımını benimsemiştir. Örneğin, Illinois Eyaleti, iş yapmak için blokzinciri kullanımına izin verilen ve blokzinciri veya akıllı sözleşmeler üzerindeki yerel hükümet kısıtlamalarını yasaklayan Blokzinciri Teknoloji Yasasını yayınlamıştır (Establishing Blockchain Policy, 2019).

ABD Genel Hizmetler İdaresi (GSA), satın alma sürecinin bazı kısımlarını otomatikleştirerek devlet satın alımını modernize etmek istemektedir (Aleksandar, t.y.) Proje ile kamu kurumlarına hizmet sunumu yapacak şirketler tarafından, akıllı sözleşmeler kullanılarak otomatik olarak incelenen ve değerlendirilen teklifler

sunulması, bu suretle işlem süresini büyük ölçüde azaltırken şeffaflığı ve doğruluğu arttırması hedeflenmiştir. Buna ek olarak, devlet blokzinciri girişimlerini ve bilgilerini izlemek için, merkezi bir portal olarak hizmet veren Gelişmekte Olan Vatandaş Teknolojisi Kurumlar Arası Blok Zinciri Programı yoluyla iş birliği ve teknolojinin benimsenmesi hedeflenmektedir.

İç Güvenlik Bakanlığı (DHS), Amerika Birleşik Devletleri altyapısını ve vatandaşlarını siber saldırılardan korumak için blokzinciri tabanlı uygulama geliştirmektedir. (Aleksandar, t.y.) Ek olarak, Hastalık Kontrol Merkezi (CDC), kritik verilere gerçek zamanlı erişimi büyük ölçüde iyileştirmek ve halk sağlığı çalışanlarının müdahale sürelerini hızlandırmak blokzinciri tabanlı çalışmalar sürdürmektedir.

Boston merkezli özel bir internet oylama şirketi Voatz tarafından 2016 yılında başlayan ve ilk blokzinciri tabanlı seçimlerin gerçekleştirildiği mobil uygulama geliştirilmiştir. (Lindman v.d., 2020). Sistem, kullanıcı hesapları oluşturmak için biyometrik bilgileri kullanır ve altyapı sunucuları Hyperledger blokzincirine dayanır ve denizaşırı ülkelerdeki ABD seçmenleri tarafından tamamlayıcı oylama için tasarlanmıştır.

4.4. Güney Kore

Güney Kore Cumhuriyeti, E-Devlet Kalkınma Endeksi ve E-Devlet Katılım Endeksi'nde (UN E-Government Knowledgebase, 2021) 2. sırada yer almaktadır. Güney Kore e-Devlet alanında blokzinciri teknolojisine ve pilot projelere büyük yatırımlar yapmıştır. 2018 yılında, blokzinciri teknolojisinin kullanım alanlarını belirleme konusunda önemli bir adım atmıştır. Bilim ve Bilgi İletişim Teknolojileri Bakanlığı (MSICT), hem endüstride hem de devlette potansiyel kullanım alanlarını görmek için blokzinciri konusunda geleceğe yönelik bir strateji geliştirmiştir. Geliştirme stratejisinde 6 pilot proje için yaklaşık 9 milyon dolar bütçe ayrılması planlamış, bu projelerin ana odak alanları tedarik zinciri yönetimi, oylama, gümrükleme hizmetleri, nakliye lojistiği, gayrimenkul alım satımı ve uluslararası e-belge yönetimi olmuştur (Young-sil, 2018).

Blokzinciri Teknoloji Geliştirme Stratejisi, MSICT için bir ilk adım olmuş ve ardından 2020 yılında Blokzinciri Teknolojisi Yayılım Stratejisi sunulmuştur. Yayılma Stratejisi, güven geliştirme, ekonomide insan temasını en aza indirme ve verimliliği

artırma gibi blok zincirin temel avantajlarından yararlanmak için blok zinciri teknolojisini yedi sektöre uyarlamayı planlamıştır (Korea Plans, 2020). Bu yedi sektör, çevrimiçi gerçek zamanlı erişilebilir oylama sistemi, deneme olarak bir bağış platformu oluşturma, blok zinciri tabanlı bireysel gelişim hesapları, enerji sektörü, dijital para birimi için pilot proje, gayrimenkul ticareti kayıtları, bazı hizmetler için müşteri hizmetleri sistemlerini birleştirmeyi içermektedir (Korea Plans, 2020).

Pilot proje olarak, Güney Kore'nin eyaletlerinden birisi olan Gyeonggi'de, eyalet hükümeti, Blocko isimli firmayla bir iş birliği içerisinde yardım projeleri için gerçekleştirilen halk oylamasında blokzinciri teknolojisini kullanmışlardır (Garrett Keirns, 2017). Özellikle, blokzinciri ve akıllı sözleşmeye dayalı oylama platformu, topluluk üyelerinin topluluk yardımı girişimleri önermesine ve oy kullanmasına olanak tanımıştır (Özaltın ve Ersoy, 2020). Eyalet hükümetine göre blok zinciri tabanlı çözüm, geleneksel temsili demokrasiyi doğrudan demokrasiyle tamamlama olasılığına izin vermiştir. (Hogan, Ojo ve Harney, 2017).

Geliştirilen başka projede, kamu kurumları ve özel sektörün yer aldığı oluşum tarafından bir DLT geliştirilmiştir. Bu DLT ile kullanıcıların kişisel verileri ve kuruma ait kişisel bilgileri kontrol etmelerini sağlayan dağıtık bir kimlik teknolojisi altyapısı geliştirilmiştir. Bu altyapıda kimlik kartı yerine mobil telefon uygulaması üzerinden kimlik tanıtım işlemleri geliştirilmiştir (Jae-yeon, 2020).

Güney Kore Hükümeti tarafından yürütülen ICON adlı pilot uygulama, belgelerin yayınlanması, değerlendirilmesi ve bilgilerin kaydedilmesi gibi idari işler için bir pilot blokzinciri projesidir (Young, 2019). Proje kapsamında bir blokzinciri yönetişim ekibi seçilmiş ve blokzinciri tabanlı bir çevrimiçi oylama platformu olan m-Voting oluşturulmuştur (Andrews, 2019). Ancak, kullanımın tüm taraflarca kabul edilmesi proje için bir zorluk olarak ortaya çıkmıştır. Blokzincirinin diğer kamu hizmetlerine uygulanması için çalışmalar devam etmektedir.

4.5. Blokzinciri Tabanlı Diğer Çalışmalar

Liu, Piao, Jiang ve Zheng (2018), farklı kamu kurumları arasında veri paylaşılırken veri koruma ihlallerine odaklanan ve işlem sırasında veri ihlallerinin nasıl korunacağını açıklayan bir veri paylaşım çerçevesi önermiştir. Bu çerçevede her bir paydaşı temsil eden düğümler arasında bilgi paylaşımı özel blokzincirler kullanılarak

yapılır, bu ağdaki düğümlerin kimliğini doğrular ve birbirlerine güvenmelerini sağlar. Sistem ayrıca kriterlere göre verileri sorgulayabilir, verilere sahip olan bölümlerin isimlerini toplar ve talep alışverişinde bulunur. Blokzinciri toplu kullanıcı mesajını sıralar ve anonimliği sağlamak için kullanıcı verilerini anonim olarak işler ve işlem tamamlandıktan sonra blokzincirine kaydedilir. Bir veri talebi olduğunda, ilk adım, istenen bilgiyi bulmak ve isteği düğüme göndermektir. İstek kabul edildiğinde, talep edilen verileri gizlilik sunucusuna depolamak için belirli bir süreç çalışır, ardından istek onaylanır ve veri paylaşımı başlar. Blokzincirinin rolü, her kullanıcının kimliğini doğrulamak ve verilerin sahteciliğini önlemektir. Doğrulama, PoW konsensüs algoritması kullanılarak yapılır.

Ghanem ve Alsoufi (2019), işlemde yer alan kuruluşlar arasında birlikte çalışabilir bir ağ oluşturulması yoluyla e-Devlet portalı tarafından sağlanan bir e-Hizmeti vaka çalışması olarak kullanmışlardır. Çerçeveleri G2C, G2B ve C2C hizmetlerinde bilgi alışverişini kolaylaştırır ve iş birliğini geliştirir. e-Devlet portalı, vatandaşlara güvenli bir şekilde hizmet talep etmek ve kimliklerini doğrulamak için kullanılan bir e-Anahtar sağlar. Blokzincirinin rolü, istenen hizmeti tamamlamak için gerekli belgeleri kontrol etmek için ilgili hizmetle ilişkili uygun akıllı sözleşmeyi belirtmektir. Toplama işlemi vatandaş tarafından onaylanmalıdır. Temel belgeler tamamlandıktan sonra akıllı sözleşme, akıllı sözleşme tarafından tanımlanan işlemi tamamlamak için ilgili hizmet sağlayıcıya belgelerin bir kopyasını toplama yetkisi verir. Yeni bir belge yayınlandığında, ağın tüm taraflarının madencilik süreci ile doğrulaması gereken blokzincirine eklenir. İlk belge, verilen kullanıcı için kullanılabilirlik ve özgünlük için hizmet sağlayıcının deposunda saklanacaktır. Tüm kullanıcılar defterin bir kopyasını tutsalar bile, hizmeti tamamlamak için yalnızca belgeyi ön izleyebilirler.

Zhang, Deng, Zhang, ve Kong (2019), blokzincirini mali, hukuk, vergi, eğitim ve tıp departmanları dahil olmak üzere farklı kamu kurumları arasında bilgi paylaşımı amacıyla bir hükümet modeli oluşturmak ve güvenlik ve güvenilirlik sorunlarını çözmek için temel teknoloji olarak değerlendirmiştir. Yazarlar, bir konsorsiyum blokzincirine dayalı uygulama stratejisini belirlemiş ve bilgi paylaşımı için çözümler ortaya koymuştur. Blokzinciri teknolojisi, düğümlerin içeriğinin değişmez olduğu, bir konsensüs eklentisinin kullanılması verilerin senkronizasyonunu garanti ettiği ve ayrıca verilerin güvenliğini sağladığı eşler arası bir ağa dayanmaktadır.

Naing (2019), güvenlik, güvenilirlik ve saydamlığı sağlamak için devletten çalışana, devletten vatandaşa, işletmeden işletmeye ve devletten devlete işlemlerini kapsayan e-Devlet hizmetleri için kullanılabilecek genel bir açık blokzinciri çerçevesi modeli önermiştir. Çalışmada tüm yetkililer arasında ortak bir veri çerçevesinin kullanılmasının da birlikte çalışabilirliği artıracağını açıklanmıştır. Önerilen genel çerçeve, beş katmana sahip dağıtık bir blokzincirine dayanmaktadır:

Elisa, Yang, Li, ve Chao (2019), geleneksel kağıt tabanlı veri paylaşım sistemini, fiziksel konumlarına rağmen vatandaşlar ve işletmeler için birlikte çalışabilir bir ortamda hizmet sağlayan elektronik muadiline dönüştüren güvenli ve merkezi olmayan bir e-devlet konsorsiyumu blokzinciri tabanlı sistem önermişlerdir. Sistemin amacı kolaylık, şeffaflık ve verimliliği sağlamak ve aynı zamanda e-Devlet hizmetlerinin kalitesini artırmaktır. Konsorsiyum blokzinciri katmanı, işlemleri doğrulamak ve ağa katılmadan önce kullanıcıların kimliğini doğrulamak için önceden seçilmiş e-Devlet düğümlerinden oluşan eşler arası bir ağdır. Ağda PoW konsensüs algoritması kullanılır ve. ağ katmanı, tüm katmanlar arasındaki bağlantıyı sağlar. Defter depolama katmanı, gelecekte silinecek veya değiştirilecek olan belgeler, resimler veya veriler gibi büyük dosyaları blokzincirinde depolamak için kullanılır. Bu katmanın gerekliliği, blokzincirinin değişmezliğinden kaynaklanmaktadır.

4.6. Türkiye'de Blokzinciri ile İlgili Gelişmeler

Blokzincirinin kamu yönetimi açısından henüz olgunlaşmamış bir teknoloji olduğu göz önüne alındığında, pilot çalışmalar bu teknolojinin avantaj ve dezavantajlarını tespit etmek açısından önem arz etmektedir. Türkiye henüz pilot test aşamasına geçmemiş olsa da genel olarak ve kamu yönetiminde blockzinciri teknolojisinin kullanımı konusunda bazı adımlar atmaya başlamıştır. Alt bölümlerde bu gelişmeler gözden geçirilmektedir.

4.6.1. Blokchain Türkiye

Türkiye Bilişim Vakfı (TBV) tarafından Haziran 2018'de kurulan Blockchain Türkiye adlı platform, Eylül 2020 itibarıyla ondan fazla farklı endüstriyel sektörden 75 üyeye ulaşmıştır (BCTR, t.y.). Platform, blokzinciri teknolojisinin ulusal potansiyelini ve kamuoyunu bilinçlendirmek amacıyla faaliyet göstermektedir. Eğitim vererek,

etkinlikler düzenleyerek, ilgili içerik üreterek ve yayınlayarak, mevcut fırsatları değerlendirerek ve blokzinciri teknolojisinin uygulanmasını sağlayarak ekosistem için stratejik öncelikleri belirlemeyi ve faydalarını değerlendirmeyi hedeflenmektedir.

4.6.2. TÜBİTAK Blokzinciri Araştırma Laboratuvarı (BZLab)

Kamu ve özel kurum/kuruluşların ihtiyaçlarına istinaden, blokzincir teknolojilerinin altyapısı, kurulumu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetlerini icra etmek üzere, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında Blokzincir Araştırma Laboratuvarı (BZLab) kurulmuştur (BZLab, t.y.)

4.6.3. 11. Kalkınma Planı (2019-2023)

Cumhurbaşkanlığı tarafından 2019 yılında hazırlanıp yayınlanan 11. Kalkınma Planı'nda (2019-2023) (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2019) blokzinciri tabanlı dijital merkez bankası parasının uygulanacağı belirtilmektedir. Blokzinciri uygulamalarının kullanımını kolaylaştırmak için ulaşım ve gümrük hizmetlerinde gerekli yasal ve fiziki altyapı projelerinin tamamlanacağı hedeflenmiştir. Ayrıca, kamu hizmetlerinin (örn. e-devlet) geliştirilmesinde büyük veri, bulut bilişim, mobil platformlar, nesnelerin interneti, yapay zeka ve blokzinciri gibi yeni teknolojilerin kullanılması için süreçlerin ve teknolojik altyapının iyileştirilmesi planlanmaktadır.

4.6.4. Ulusal Blokzinciri Altyapısının Kurulması

Sanayi ve Teknoloji Bakanlığı tarafından geliştirilen 2023 Sanayi ve Teknoloji Stratejisi'nde (T.C. Sanayi ve Teknoloji Bakanlığı, 2019);

- Ulusal blokzinciri altyapısının geliştirilmesi, yeni ve gelişmekte olan bir teknoloji olan blokzinciri tabanlı bir ağ oluşturulması,
- Blokzinciri teknolojisi konusunda uygulama geliştirme yetkinliğine sahip olmak için tüm kamu merkezli başvurular (tapu kaydı, diploma, gümrük başvuruları vb.) "Açık Kaynak Platformu" girişimi kapsamında belirlenmesi ve projelendirilmesi,

- Yeni, güvenli iş modeli ve süreçlerinin (tedarik zinciri, bankacılık, yasal takip uygulamaları vb.) test edilmesi için geliştirilen blokzinciri altyapısında, pilot uygulamalar için bir test ortamı ve katılımcı kümesi oluşturulması,
- Geliştirilen blockchain uygulamalarının uyumluluk testleri için düzenleyici komite ile birlikte bir "düzenleyici sandbox" oluşturulması, testleri başarıyla tamamlayan girişimlerin belgelendirilmesi ve yatırımlarına destek verilmesi hedeflenmiştir.

4.6.5. Diğer Çalışmalar

UEKAE, blokzinciri tabanlı Yeni Nesil Merkezi Olmayan Dijital Kimlik Altyapısı (MODKA) üzerinde çalışmaya devam ediyor (Intersessional panel, 2020). Bu altyapı, mevcut kimlik sistemleri ve diğer altyapılarla entegre edilerek Türkiye'nin gelecekteki ulusal dijital kimlik yönetimi omurgası olarak kullanılabilecektir.

Blokzincirini Türkiye'de yaygınlaştırmak için Blokzinciri ve Araştırma Ağı (BAG) platformu kurulmuştur (Intersessional panel, 2020). Amacı blockchain teknolojisi ile ilgili konularda Ar-Ge faaliyetlerini kolaylaştırmak ve Ar-Ge yapmak isteyen araştırmacıların birlikte çalışmasını sağlamaktır.

TAKASBANK'ın altına dayalı kripto para geliştirme projesinde (BİGA) sistemin saha testleri yapılmıştır. Yakın gelecekte yaygınlaşacağı düşünülen Merkez Bankası Dijital Para biriminin tasarımı konusunda akademik çalışmalar yürütülmekte, ancak çok daha kapsamlı çalışmalara ihtiyaç bulunmaktadır (Intersessional panel, 2020).

Bu bölümde dijital devlet bağlamında dünyadaki blokzinciri strateji, politika ve uygulamaları ile Türkiye’nin mevcut durumu ele alınmıştır. Sonraki bölümde Türkiye’de dijital devlet yapısı içerisindeki paydaşlar arası etkileşim sorunları ve bu bölümde ele alınan örnekler doğrultusunda blokzincirinin bu maksatla kullanılabilirliği incelenmiştir.

5. TÜRKİYE'DE DİJİTAL DEVLET PAYDAŞLARI ARASINDAKİ ETKİLEŞİM SÜREÇLERİNDE BLOKZİNCİRİNİN KULLANILABİLİRLİĞİ

5.1. Paydaşlar Arası Etkileşim Süreçlerinde Karşılaşılan Başlıca Sorunlar

Dijital devlette paydaşlar arası bilgi paylaşımı ve farklı devlet kurumlarının sistemlerinin entegrasyonu; veri girişinden ve diğer sorunlardan kaynaklanan veri kalitesi, web hizmetlerinin ve verilerin kendisinin yetersiz belgelenmesi, kuruluşlar arasında verilerin standardizasyonu, teknik düzeydeki sorunlar nedeniyle bazı zorluklara sahiptir. Tüm bu sorunlar entegrasyon süreçlerinin uzamasına ve kaçınılmaz veri yorumlama hatalarına neden olarak vatandaşların mağdur olmasına neden olmaktadır.

Diğer gelişmekte olan ülkelerde olduğu gibi, Türkiye'de de e-Devlet bağlamında birlikte çalışabilirlik ve eşgüdüm sorunları, diğer bir deyişle paydaşlar arası etkileşim süreçlerinde karşılaşılan başlıca engeller aşağıdaki şekilde sıralanabilir.

5.1.1. BİT Altyapısı

BİT altyapısı, bilgi paylaşımını ve paydaşlar arasındaki iletişimi engelleyen, dolayısıyla bilgi sistemleri birlikte çalışabilirliğini ve çevrimiçi hizmet sunumunu etkileyen ana engellerden biri olarak belirtilmektedir (Paul ve Paul, 2012; Solli-Saether, 2010). Gelişmekte olan ülkelerde olduğu gibi, Türkiye de uygun BİT altyapısını tasarlamada birçok sorunla karşı karşıyadır. Dijital projelerinden maksimum faydayı elde edebilmek için, devletin BİT sektöründe güncel ve son teknoloji ile uygun BİT altyapısı geliştirmesi gerekmektedir.

5.1.2. Veri ve Bilgi Entegrasyonu

Veri entegrasyonu, farklı devlet kurumları içinde veri ve bilgi alışverişini kolaylaştırır ve paydaşlar arası etkileşimde önemli bir faktör olarak sınıflandırılır. Veri entegrasyonu, kurum içinde ve diğer devlet kurumlarıyla ortak veri tanımları, veri bakımı ve bilgi yönetiminden etkilenir (Paul ve Paul, 2012; Petter, DeLone ve McLean, 2008). Veri entegrasyonu, ortak veri ve birleşik veritabanı konsept yönetim sistemleri kullanılarak bilgi standardizasyonuna bağlıdır. Standartlaştırılmış

yönergeler, e-Devlet birlikte çalışabilirliğine ulaşmanın etkili yolları olarak kabul edilir. Veri tutarsızlığı ve bilgi kalitesi, veri ve bilgi entegrasyonu için büyük bir zorluk olarak kabul edilmektedir (Klischewski ve Scholl, 2006).

5.1.3. Güvenlik ve Mahremiyet

Farklı devlet kurumları, güvenlik ihlallerinden kaynaklanan mahremiyet ve kişisel verilerin korunmasına ilişkin yasa nedeniyle bilgi sistemi paylaşımına hala düşük güven duymaktadır (Sohimi ve Abbas, 2011). Güvenlik standartları, sızıntı testleri ve gizlilik rolleri uygulamak, devlet kuruluşlarını kendi aralarında veri paylaşmaya ve kurumsal düzeyde etkileşimi artırmaya yönlendirir.

5.1.4. İş Süreçleri

Devlet hizmetlerinin vatandaşlara sunulması, çeşitli operasyonel prosedürlerden ve kurumlar arası hizmetler olarak da tanımlanan departmanlar arası iletişimden geçer. Bazı süreçler, hizmeti sunmak için birçok devlet kurumunu içerir (Paul ve Paul, 2012; Solli-Saether, 2010). Paydaşlar arası etkileşim süreçlerini geliştirmek, iş tekrarından kaynaklanan gereksiz bileşenleri hariç tutmak için iş süreçlerinin yeniden yapılandırılması yoluyla yapılabilir. İş süreci bilgi sistemleri birlikte çalışabilirliği, devlet kurumlarının yeni ve mevcut hizmet sunum gereksinimlerine yanıtını iyileştirir. Bu, iş gereksinimleri ve iş süreçleri yönetimine ilişkin ortak bir anlayışın geliştirilmesiyle mümkün olur. Bu, iş süreçlerinin yeniden yapılandırılmasıyla elde edilen etkileşim yöntemleri aracılığıyla devlet kurumları içinde gelişmiş işbirliğine yol açar (Stemberger ve Jaklic, 2007).

5.1.5. Standardizasyon

E-Devlet sürecinde karşılaşılan engellerden birisi de kurumsal yapılanmalarda ve sistemler arasında bir takım standartların olmayışıdır. Kamu kurumlarının birbirlerinden bağımsız şekilde geliştirdikleri e-devlet projelerinde kurumlar arasında veri paylaşımında sorunların yaşanmasına yol açabilecek durumlar; verilerin tanımlanma şekillerindeki farklılıklar, sistemlerde farklı ve birbirleriyle uyumsuz yazılımların kullanılmış olması, bilgilerin güvenliği, gizlilik ve kimlik doğrulama gibi konularda belirli bir standardın olmayışı ve farklı kurumsal mimari ve teknik standartların varlığı vb. şeklinde sıralanabilir (Seferoğlu, Çelen ve Çelik, 2011)

5.1.6. Üst Yönetim Desteği

Yeni projelere başlarken kritik faktör olarak kabul edilir. Gerçek maliyet ve faydalara odaklanmak, herhangi bir yeni e-Devlet projelerinin planlama aşamasında üst yönetimin endişesidir. Proje yönetimi aşamaları öncesinde, sırasında ve sonrasında motive etme, etkileme ve liderlik etme yoluyla destekleri kritik öneme sahiptir ve bu nedenle varlığının olmaması büyük bir engel haline gelir. Finansman, destek, konsept açıklama ve üst yönetimden farkındalık projenin başlangıcından önce gelirken, üst yönetimin herhangi bir değişikliği kontrol etmek için yönetim desteği e-Devlet uygulaması sırasında gelir. Sorunsuz çalışmayı desteklemek ve projenin doğru yolda olmasını sağlamak için proje bittikten sonra bile üst yönetimin rolü artar (Melitski ve diğerleri, 2011). e-Devlet projelerinin tüm aşamaları, bu projelerin belirlenen çerçevede başlatılmasını, yaygınlaştırılmasını ve uygulanmasını sağlamak için üst yönetim desteğinden etkilenir. Farklı devlet kuruluşları arasındaki üst yönetim koordinasyonu, kurumsal düzeyde etkileşimi kolaylaştırır ve bu kuruluşlar arasındaki boşluğu en aza indirir.

5.1.7. İnsan Kaynakları

Devlet sektöründeki BİT becerilerinin eksikliği, birlikte çalışabilirliğinin zorluklarından biri olarak kabul edilebilir. BİT sektöründe nitelikli ve iyi eğitilmiş insan kaynakları eksikliği, gelişmekte olan ülkelerin karşılaştığı temel sorun olarak gösterilmektedir. e-Devlet programında birlikte çalışabilirliğinin başarısı, büyük ölçüde hükümette uygun BİT becerisinin mevcudiyetine bağlıdır. BİT altyapısını analiz etmek, tasarlamak, kurmak, uygulamak ve sürdürmek ve ayrıca çevrimiçi e-hizmetleri yönetmek için yetişmiş insan kaynaklarına ihtiyaç vardır. (Hellman, 2010).

5.2. Blokzincirinin Paydaşlar Arasındaki Etkileşim Süreçlerinde Kullanılabilirliği

Hükümetlerin maliyet etkinliği ve hesap verebilirliğe odaklandığı ve bu hususları sağlam politika oluşturmanın temel özellikleri olarak gördüğü bir dönemde, blokzinciri teknolojisinin kamusal alandaki bir dizi zorluğa olası çözümlerinin veya çalışma alanlarının ortaya konması gerekmektedir. Halihazırda üçüncü bölümde incelenen vaka çalışmalarından blokzinciri teknolojisinin kamu hizmetine aşağıdaki

faydaları sağlama potansiyeline sahip olduğunu söylemek mümkündür (Berryhill, Bourgery ve Hanson, 2018):

- Etkinliği artırmak,
- Kurumlar arasındaki uyuşmazlıkları azaltmak,
- Bürokratik engelleri azaltmak,
- Bilgiyi daha iyi paylaşmak
- Akıllı sözleşmeler yoluyla otomasyonu teşvik etmek.

Bu noktadan hareketle, blokzinciri teknolojisinin geleceği hakkında belirleyici iddialarda bulunmak veya nerede ve tam olarak nasıl kullanılması gerektiği konusunda net önerilerde bulunmak mümkün olmamaktadır. Yapılabilecek tek açık tavsiye, hükümetlerin bu teknoloji hakkındaki bilgilerini geliştirmeye yatırım yapmaları ve olası uygulamalarını keşfetmeleri ve hatta denemeleri gerektiğidir.

Şeffaflık, verimlilik, veri bütünlüğü ve güvenlik gibi blokzincirinin avantajları, kamu sektörüne de fayda sağlayacağı değerlendirilmektedir. Spesifik olarak, ademi merkeziyetçilik özelliği, tüm paydaşlar için daha adil bir ortam sunarak birden fazla kurum arasındaki etkileşim süreçlerini iyileştirebilir. Aynı şekilde, birbirine tam olarak güvenmeyen veya bilgileri doğrulamak için herhangi bir merkezi otoriteye güvenmeyen taraflar arasında doğrudan, eşler arası veri yönetimine olanak sağlayabilir. Bu nedenle, blokzinciri ilgili çeşitli güç dinamiklerinden bağımsız olarak etkileşim süreçlerini iyileştirmek için yeni bir yol olabilir.

Blokzinciri teknolojisi bu nedenle belirli bir ağın katılımcılarının belirli bir karşılıklı güvene sahip olmadığı durumlarda bile merkezi sistemlerin sorun alanlarını gidererek merkezi olmayan ve güvenli sistemlerin oluşturulmasını sağlar. Blokzincirinin bu benzersiz özellikleri, aynı zamanda dijital pazardaki mevcut bazı oyuncuların veri tekelinin üstesinden gelmek amacıyla, merkezi olmayan sistemler geliştirmeyi (Wessling, Ehmke, Hesenius ve Gruhn, 2018) amaçlayan çok sayıda girişimi teşvik etmiştir (Yano, Dai, Masuda ve Kishimoto, 2019).

Bununla birlikte, dijital devlet bağlamında bazı uygulama girişimlerine rağmen, bu teknolojinin yaygın kullanımı ve uygulanması bazı zorluklar içermektedir ve blokzinciri kamu sektöründeki her soruna bir çözüm değildir.

Çoğu kamu idaresinde BİT sistemi merkezi bir mantığa göre uygulanmaktadır. Bu durum, merkezi olmayan bir paradigmaya geçişi engellemese bile yavaşlatabilir. Değiştirme maliyetleri, merkezi olmayan sistemlerin yaygın kullanımına büyük bir engel oluşturabilir. Bir BİT sisteminin yeniden düzenlenmesinin maliyetler gerektirdiği ve başarısızlıklara yol açabileceği dikkate alınmalıdır (Roman, 2013). Sonuç olarak, kamu kurumlarındaki karar vericiler, özellikle ödenekler yoksa veya çok azsa, bu yenilik için kamu kaynağını israf etme riskinden kaçınmayı tercih edebilirler.

Blokzincirinin başlangıçta merkezi bir yönetim otoritesine sahip olma ihtiyacını ortadan kaldırmak amacıyla tasarlandığı da dikkate alınmalıdır (Xu ve diğerleri, 2019) Aslında, bu tür bir düzenleme kapasitesi, blokzincirinin Bitcoin'den başlayarak kripto para birimi sektöründe oldukça popüler hale gelmesine olanak sağlamıştır. Adalet Divanı'nın 22 Ekim 2015 tarihli ve C-264-14 sayılı içtihadıyla da onaylandığı üzere, Bitcoin "tek bir ihraççıya sahip değildir ve bunun yerine doğrudan bir ağda özel bir algoritma ile oluşturulur". Bu, bir tür kuruluşun normalde bir kamu çıkarını elde etmek için yetkilere sahip olduğu modern kamu hukuku sistemleriyle tam bir tezat oluşturmaktadır (Goodnow, 1983). Bu, tek başına blokzinciri teknolojisinin kamu sektöründeki faydası konusunda şüphe uyandırabilir.

Blok zincirlerinin en çok tartışılan faydalarından biri, merkezi bir otorite ihtiyacını ortadan kaldırabilmeleridir. Ancak, herkesin erişebileceği ve işlem yapabileceği izinsiz defterler için bile bu tamamen doğru değildir. Blokzincirleri yoktan var olmaz; blokzinciri platformunun geliştirilmesi için kilit rollere sahip kod geliştiriciler, mühendisler ve diğer karar vericiler tarafından inşa edilmeli ve yönetilmelidirler. Bu geliştiriciler fiili bir merkezi otoritedir ve bunların bileşimi, eylemleri ve bir blokzincirine kodlanmış temel kararları, işlemlerin kendileri kadar şeffaf olmayabilir. Bu önemli bir soruyu gündeme getirmektedir.

Blokzincirinin meşru yönetim kuruluşu kim veya ne olacak, kamuya açık mı veya özel mi olacak? Sivil toplum tarafından kamusal yaşamın tüm alanlarında daha fazla hesap verebilirlik talep edildiğinden, blokzincirini kimin kontrol edeceğine dair kararlar önemlidir. Karar verme seviyeleri ve bu tür kararların platformun koduna entegrasyonu, bu nedenle önceden hazırlanmış olan koda bağlıdır. Güç dinamikleri, hatta kamu alanı blokzincirlerinde bile, nihayetinde her bir platformun kodunun izin verdiği şeyle sınırlıdır. Sonuçta, gerçek kodlama uygulaması dış kaynaklı olsa bile,

ortaya çıkan blokzinciri ürününün uygunluğunu sağlamak ve sorumluluğunu üstlenmek için kamu kurumlarının kodlama sürecine dahil olmasını gerektirecektir. Ek olarak, hükümetler blokzinciri teknolojilerini kullanmaları için yönetişim yapılarını ve bunlara giren kararları dikkate almalıdır. Bu, devlet çapında blokzinciri stratejileri ve kullanımları hakkındaki üst düzey kararlardan, bireysel blokzinciri protokollerini, ağlarını ve uygulamalarını tasarlamak ve uygulamak için yönetişim ve izinlere kadar uzanır.

Değişmezlik, blokzinciri teknolojilerinin en temel özelliklerinden ve faydalarından biridir, ancak pratik uygulanabilirlik açısından belki de en büyük sınırlamasıdır. Günümüzde kamu sektörünün kullandığı geleneksel veritabanlarından farklı olarak blokzincirine girilen verileri kaldırmanın bir yolu yoktur. Verilerin güncellenmesi ve/veya silinmesinin olağan olduğu durumlarda, blokzinciri teknolojisini kullanmak en iyi seçenek olmayabilir. Karar vericilerin, blokzincirlerini kullanmanın faydalarının, verileri güncelleme ve silme yetersizliğinden daha ağır basıp basmadığına karar vermeleri ve kullandıkları veri türü için değişmezliğin pratik olup olmadığını kendilerine sormaları gerekir (Yaga, Mell, Roby ve Scarfone, 2018).

Diğer yandan, kişisel verilerin korunmasına ilişkin mevzuatın artan önemi göz önüne alındığında, bu disiplinin kamu sektöründe blokzinciri kullanma olasılığını sınırlayıp engelleyemeyeceğini ve nasıl sınırlayacağını değerlendirmek gerekir.

İzinsiz blokzincirleri, "merkezi olmayan mimarilerin genellikle herkesin etkileşimlerinin açıklanmasına dayandığı" (Filippi, 2016) şeffaflığa izin verir. Gizlilik ayarları yok denecek kadar azdır. Ancak, kişisel bilgilerin saklanmasının daha olası hale geldiği bir zamanda gizlilik ve mahremiyet mekanizmaları büyük önem taşımaktadır. Kurallar ve yasalar, bu tür bilgilerin mutlak korunmasında ısrar eder. Örneğin, AB'nin unutulma hakkı ilkesi, bir bireyin, potansiyel olarak bazı devlet kayıtları da dahil olmak üzere, kendisiyle ilgili bilgilerin kaldırılmasını talep edebileceğini şart koşar (Gabison, 2016). Değişmezliği nedeniyle, bir kişi hakkındaki bilgiler bir blokzincirinde saklanıyorsa, unutulma hakkı esasen uygulanamaz. Ancak, vatandaşların bilgilerinin tüm devlet veritabanlarından kaldırılmasını talep etme hakkı bulunmadığından, bu sorun yalnızca belirli durumlarda kamu alanı ile ilgili olabilir. Örneğin hiç kimse devletten kimlik bilgilerinin veya adli sicil kayıtlarının silinmesini isteyemez. Sadece unutulma hakkının belirli uygulamaları geçerli olabilir. Ek olarak,

çoğu olmasa da, blokzinciri teknolojisinin kamu uygulamalarının çoğu, kamu görevlilerine erişimi kontrol etme yeteneği veren izinli defterler olacaktır.

Merkezi olmayan karar verme düzeyleri ve mahremiyet arasında gerekli bir dengeleme yapılması gerekecektir. "Radikal şeffaflık" (Filippi, 2016) kişisel verilerin istismarına yönelik riskler getirebilirken, daha yüksek düzeyde gizlilik daha resmi yönetişim modelleri (izin verilen blokzincirleri) gerektirecektir, ancak blokzinciri teknolojisinin temel amacına daha yakın olmaya devam etmektedir. Kamu kurumları ayrıca hangi bilgilerin bir blokzincirinde saklandığını ve bu nedenle değişmez olduğunu ve hangi bilgilerin zincir dışında saklandığını, belki de sadece blokzincirinde bulunan bir bağlantı veya referans ile kullanımını değerlendirmesi gerekebilir. Kamu kurumlarının, blokzincir teknolojilerini geliştirme sürecinde teknik düzeyde mahremiyeti dikkate almaları gerekmektedir.

Kamu ve özel sektör kuruluşları, diğer paydaşlar belgeler, resimler, videolar ve uygulamalar biçimindeki büyük miktarda veriyi depolamak için genellikle veritabanlarını kullanır. Bir blokzinciri genel olarak bir işlem listesidir ve en fazla akıllı sözleşmeleri yürütmek ve yönlendirmek için kullanılan küçük veri bloklarını içerir; genel veri depolama için tasarlanmamışlardır. Bununla birlikte, büyük miktarda veri blokzinciri dışında saklanabilir ve bir blok işlemi içinden bağlanabilir. (Yaga ve diğerleri, 2018). Kamu kurumları yalnızca veri depolama arıyorsa, blokzinciri teknolojisi en uygun olmayabilir. Bununla birlikte, dağıtılmış ve güvenilir bir işlem kaydı tutmanın bir yolunu arıyorlarsa, blokzinciri teknolojisi uygun bir çözüm olabilir. Hem blokzinciri teknolojisinin hem de bir veri depolama çözümünün takip edildiği, blokzinciri işlemlerini zincir dışında tutulan ve başka bir yerde depolanan verilerle ilişkilendirme yeteneği sağlayan hibrit bir yaklaşımın uygulanması mümkündür.

Diğer bir anlatımla verilerin bütünlüğünü ve gerçekliğini garanti edebilecek küçük bilgi parçaları blokzincirine kaydedilebilir. Örneğin, bir zaman damgasıyla birlikte onaylanacak verileri temsil eden bir karma, belirli bir belgenin belirli bir anda belirli bir içeriğe sahip olduğunu garanti etmek için bir blokzincirinde saklanabilir. Bu durumda da belge içeriğini blokzincirine kaydetmeye gerek kalmadan herhangi bir yerde depolanabilir. Daha sonra da herhangi bir zamanda, bu belgenin bütünlüğü, blokzincirinde saklanan parmak izi kontrol edilerek doğrulanabilir.

Blokzincirleri birden fazla paydaşın belirli bir kamu gücünü kullanmak için etkileşime girmesi gerektiğinde, kurumlar arasında bilgi alışverişi, her bir kuruluşun kendi yetkinliğine sahip verileri saklama hakkına sahip olduğu özel blokzincirler sayesinde ve ayrıca işlevsel olan diğer kamu kuruluşları tarafından saklanan veri kümelerine erişim sayesinde gerçekleşebilir. Merkezi bir sisteme göre avantaj, merkezi bir toplama noktası sağlama ihtiyacını ortadan kaldırarak tüm düğümlerin, yani dahil olan tüm idarelerin eşitliği olacaktır.

Alternatif olarak, bir idarenin bir kişinin verilerini veri tabanına kopyalamak ve böylece kullanıcının kişisel verilerini ve ilgili riskleri çoğaltmak yerine, birden fazla diğer kamu kuruluşundan kontrol etmesi gerekiyorsa, yalnızca bu tür verileri tanımlayan karmaları kaydedebilir. Bu şekilde kurumlar, bu işlem bir kez yapıldığında, verileri veritabanlarına kaydetmeye gerek kalmadan faaliyetlerini onaylayabilir. Sonuçları daha sonra doğrulamak için, diğer varlıkların veritabanlarında bulunan orijinal verilerle blokzincirine kaydedilen hashleri geçmek yeterli olacaktır. Bu şekilde, blokzincirine ve üçüncü tarafların veritabanlarına erişimi olan herkes, herhangi bir zamanda, birden fazla yerde çoğaltmak zorunda kalmadan verilerin doğruluğunu kontrol edebilir.

Blokzincirlerinin, kamuya açık verilerin özel kişilerle paylaşılmasında daha fazla şeffaflığa izin verebileceği de öngörülebilir. Bu, kamu otoritesinin verilerin güncellenmesi üzerinde kontrolü elinde bulundurduğu ve kişilerin bunlara anında ve doğrudan erişmesine izin verdiği, kamuya açık izinli blokzincirleri aracılığıyla yatay bir veri dağıtımı sayesinde gerçekleşebilir. Bu durumda, merkezi sistemlere göre avantaj, bir blokzinciri tabanlı sistem, vatandaşların gerekli bilgilerin ortak koruyucuları olmalarına ve böylece verilere erişime izin vermeyi amaçlayan hizmetlerin aracılığı olmadan doğrudan erişmelerine izin verecektir.

Bununla birlikte, blokzincirine kaydedilecek verilerin küçük bilgi parçalarından oluşacağını bir kez daha vurgulamak gerekir. Bu nedenle, önceki örneklerde olduğu gibi, en olası senaryo, blokzincirinin yalnızca kamuya açıklanacak verilerin karmalarını depolaması olacaktır. Gerçek bilgi daha sonra blokzincirinden daha verimli araçlarla değiş tokuş edilir.

Son olarak, dağıtık veri tabanının birlikte oluşturulmasına kişilerin de belirli bilgileri kendileri girerek katılma olasılığını düşünmek de mümkündür. Bu, kamu kurularının

vatandaştan veri alması gerektiğinde yararlı olabilir. Bu, ele alınan çeşitli durumlarla ilgili olarak girilen bilgilerin yeterli düzeyde kimlik doğrulamasını sağlayarak, genel veya özel blokzinciriler aracılığıyla yapılabilir. Bu, yönetimlerin ihtiyaç duydukları bilgileri, dağıtık defterde gerçekleştirilen tüm işlemlerin tam izlenebilirliği de dahil olmak üzere blokzinciri sisteminin sağladığı değişmezlik garantisi ile elde etmelerini sağlayabilir.

6. SONUÇ VE ÖNERİLER

6.1. Sonuç

Bu çalışmanın amacı, blokzinciri teknolojisi ve dijital devlet açısından uygulama alanlarını incelemek ve Türkiye'de dijital devlet paydaşları arasındaki etkileşim süreçlerinde blokzincirinin kullanılabilirliğini değerlendirmektir. Bu amaçla blokzinciri ve özellikleri incelenmiş ve literatür taraması yapılmıştır. Kapsamlı bir bakış açısı sağlamak için öncelikle blokzincirinin yapısı ve nasıl çalışıldığı incelenmiştir. Ardından blokzincirinin dijital devlet bağlamında kullanımına ilişkin literatür taranmış ve uygulama örnekleri gözden geçirilmiştir. Bu bulgular ışığında bu bölümde Türkiye'de dijital devlet paydaşları arasındaki etkileşim kapsamında kullanımı için çıkarımlar tartışılmış, sağlayabileceği avantaj ve fırsatlar ile uygulamada yaratabileceği dezavantaj ve kısıtlamalar sunulmuştur.

Finans alanında bir teknoloji olarak ortaya çıkan blokzinciri teknolojisi, sahip olduğu özellikler ile birçok alanda dönüşümün yolunu açmıştır. Kamu yönetiminde uygulanmasına ilişkin çalışmalar, devletin mahremiyet, güvenlik, yönetişim, şeffaflık ve hesap verebilirlik gibi kavramlar etrafında toplanmaktadır. Birçok ülke, blokzinciri teknolojisi ile ilgili politikalarını şekillendirmeye ve dijital kimlik, kayıtlar, dijital para birimi, tedarik zinciri yönetimi, sağlık, eğitim gibi kamu hizmetlerine uygulanabilirliğini araştırmaya ve pilot uygulamalarla test etmeye devam etmektir. Estonya ve Güney Kore gibi bazı ülkeler pilot çalışmaların ötesine geçerek blokzinciri teknolojisini kamu hizmetlerine fiilen uygulamaktadır. Bu çalışmalar ve pilot uygulamalar erken dersler sunsa da kavram kanıtlarının veya küçük pilot uygulamaların ötesine geçen ve kamu sektöründe yenilikler sunan bir proje ortaya çıkmamıştır (Lindman v.d., 2020). Diğer bir deyişle, blokzinciri projelerinin şimdiye kadar kamu sektörü açısından erken dönemde olduğu görülmüştür.

Türkiye'deki blokzinciri uygulamaları dijital devlet kapsamında değerlendirildiğinde bazı adımlar atıldığı görülmüştür. Blokchain Türkiye Platformu, TÜBİTAK Blokzinciri Araştırma Laboratuvarı bunlardan bazılarıdır. Ayrıca 11. Kalkınma Planı ve 2023 Sanayi ve Teknoloji Stratejisi'nde, blokzinciri kullanımı destekleyecek strateji ve politikalar dikkat çekmektedir. Buna karşın dijital devlet bağlamında birlikte çalışabilirliğe ilişkin çalışma veya pilot uygulamanın olmadığı, bu nedenle

Türkiye'nin blokzincirinin kamusal alanda uygulanması açısından erken dönemde olduğu tespit edilmiştir.

6.2. Öneriler

Blokzinciri teknolojisi ile ilgili Türkiye'de yapılan çalışmaların yaygınlaştırılması, özellikle dijital devlet bağlamında pilot uygulamaların kısa zamanda hayata geçirilmesi, bu teknolojiye adaptasyonu arttıracaktır. Bunun için yapılabilecek en açık öneri, Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin koordinesinde, Dijital Türkiye Platformu çatısı altında bulunan tüm paydaşların bu teknoloji hakkındaki bilgilerini geliştirmeye yatırım yapmaları ve olası uygulamalarını keşfetmeleri ve hatta denemeleri gerektiğidir. Bu da Türkiye Blokzinciri Platformu, TÜBİTAK Blokzinciri Araştırma Laboratuvarı, özel bilişim şirketleri ve üniversiteler arasından ortaklar belirlemek ve işbirliği yapmak suretiyle yürütülmelidir.

Kamu sektöründe kurum içi teknik yetenek şu anda düşük ve blokzincirinin kısa ve orta vadeli uygulamalarının çoğunun dış kaynaklı olması muhtemel olsa bile, kaynakların verimli ve güvenli bir şekilde ele alınmasını, blokzinciri teknolojilerine kodlanmış temel varsayımların ve kararların anlaşılmasını ve istenen etkiyi elde etmesini sağlamak için kurum içi bilgi seviyesini yükseltmek kritik öneme sahiptir. Teknik yetenek sadece teknolojik bilgi seviyesi değildir. Blokzinciri teknolojisinin e-Devlet bağlamında kullanılabilirliğinin başarı şansını en üst düzeye çıkarmak için, organizasyonel ve anlamsal birlikte çalışabilirlik açısından araştırılması, buna ilişkin tasarım kararları verilmesi önemlidir.

Genel olarak, kamu kuruluşlarının dijitalleşme faaliyetlerinde ve dijitalleşme çabalarının (dijital olgunluk) faydalarından yararlanmada iyileştirme için her geçen gün yeni teknolojik gelişmeler yaşanmaktadır. Blokzinciri teknolojileri genellikle bir kuruluşa girebilecek diğer teknolojilerle aynı karmaşık altyapılar ve işletim ortamlarıyla karşılaşır. Ancak, mevcut veya eski teknolojiler ve süreçler genellikle yeni çabaların önüne geçer. Blokzincirinin e-Devlet kapsamında etkileşim maksadıyla kullanılabilirliği; açık, başarılı kullanım senaryoları ve kamuya açık olarak belgelenmiş, halihazırda uygulanma aşamasında olan ve güvenilir kullanıcı tabanları büyümüş projeleri esas alarak araştırmalıdır.

Önemli bulgulardan biri, Türkiye'de e-Devlet alanında henüz blokzinciri ile ilgili herhangi bir pilot çalışma veya kavram kanıtı yapılmamış olmasıdır. Pilot çalışmalar yapmak, bir yeniliğin olumlu ve olumsuz etkilerini ortaya çıkarmakta, böylece büyük ölçekli uygulamaların sonuçlarını tahmin etmek ve ölçmek kolaylaşmaktadır. Bu nedenle Türkiye'de kavram ispatı ve pilot çalışmaların yapılması blokzinciri ve BİT uygulamaları için önem arz etmektedir.

Ülke analizleri, pilot çalışmaların ve kavram kanıtlarının blokzinciri uygulamasında veri tabanlı politika oluşturma araçları olarak benimsendiğini göstermektedir. Ayrıca ulusal bir stratejiye sahip olmak ve bu teknoloji için donanımlı özel bir iş gücü geliştirmek de etkili girişimler olarak görünmektedir. Kamu sektörü araştırmaları ve uygulamaları açısından bu teknolojinin emekleme aşamasında olduğu göz önüne alındığında, bu yeniliğin erken dönem başarılı uygulamalarının ihraç edilebileceği, bu suretle katma değer sağlanabileceği değerlendirilmelidir.

Blokzincirlerin karakteristik özellikleri gereğince gizlilik, mahremiyet ve kişisel verilerin korunması açısından çekincelerin göz önüne alınması, e-Devlet kapsamındaki pilot ve genel uygulamaların hukuksal yönden çok iyi araştırılması ve uygulama öncesi kullanım alanları detaylı olarak tartışılmalıdır.

Blokzinciri teknolojisi, bir listenin güvenilir olmasını sağlayan birçok teknik özelliğe sahip, basitçe devam eden, değişmez ve dağıtılmış işlem listeleridir. Gelecekte, merkezi otoritelerin blokzinciri teknolojileri bağlamında rolleri, her işlemin merkezinde olmak yerine merkezi olmayan hizmetler için bir platform ve yönetişim sağlamaya geçebilir. Bu nedenle blokzincirlerine sadece teknolojik açıdan bir yenilik olarak bakmaktan öte, kamu yönetimi ve kamu politikaları alanındaki çalışmalarda, olası uygulamaların kamunun rolünü nasıl etkileyeceğine de odaklanılmalıdır.

6.3. Gelecek Çalışmalar

Bu araştırmada, dünya genelinde e-Devlet bağlamında blokzinciri kullanımının bir incelemesi ve bu teknolojinin Türkiye'de uygulanması hakkında bir analiz yapılmıştır. Çalışma, aynı zamanda Türkiye'de e-Devlet'in mevcut durumuna genel bir bakış açısı sunmaktadır. Türkiye'de vaka çalışmaları ve izleklerin başlatılması bu çalışmaya dayalı olarak geliştirilebilir.

Gelecekteki araştırmalar için, blokzincir teknolojisi e-Devlet kapsamında belirli bağlamlarda ayrıntılı olarak tartışılabilir. Yönetişim, şeffaflık, siber güvenlik, teknolojinin entegrasyonu ve entegrasyonun temelleri belirli projeler ve bölümler kapsamında incelenebilir.

KAYNAKLAR

Aleksandar, Z. (t.y.). Blockchain: Now a Reality and Rising Rapidly in the Public Sector. Erişim adresi: https://www.publicissapient.com/insights/blockchain-now-a-reality. Erişim tarihi: 25.05.2022

Alender, A., 2016. What is Estonian e-Residency and how to take advantage of it? Erişim adresi: https://www.leapin.eu/articles/e-residency. Erişim tarihi: 15.05.2022

Alharby, M., ve Van Moorsel, A. (2017). Blockchain-Based Smart Contracts : a Systematic Mapping Study. ArXiv, 125–140. https://doi.org/10.5121/csit.2017.71011

Allessie, D., Sobolewski, M., ve Vaccari, L. (2019). *Blockchain for digital government: An assessment of pioneering implementations in public services* (No. JRC115049). Joint Research Centre (Seville site).

Alshehri, M. and Drew, S. (2010). E-Government Fundamentals. IADIS International Conference ICT, Society and Human Beings.ISBN: 978-972-8939-20-5

Andrews, J. (2019). Seoul: The Blockchaın City. Cities Today. Erişim adresi: https://cities-today.com/seoul-the-blockchain-city/. Erişim tarihi: 30.05.2022

Antonopoulos, A. M., (2017). *Mastering Bitcoin*. Published by O'Reilly Media, Inc.

Avrupa Komisyonu, (2018). European countries join Blockchain Partnership. Erişim adresi: https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership Erişim tarihi: 15.01.2022

Avrupa Komisyonu, (2020). European Blockchain Services Infrastructure. Erişim adresi: https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi Erişim tarihi: 15.01.2022

Avrupa Komisyonu, (t.y.). Blockchain Strategy. Erişim adresi: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy. Erişim Tarihi: 15.01.2022

Bache, I. (2000), "Government within Governance: Network Steering in Yorkshire and the Humber", Public Administration, Vol.78, No.3, ss.575- 592.

Baran, P. (1964). On distributed communications: *I. Introduction to distributed communications networks*. Rand Corp Santa Monica Calif.

Bashir, I., (2017). Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks. Packt Publishing Ltd.

BCTR. (t.y.). Blockchain Türkiye Platformu. https://bctr.org

Bensghir, T. K. (2008). "e-Devlet Kuramsal ve Kavramsal Çerçeve". N. F. Kunduracı (Editör), e-Devlet Semineri Kitabı. Ankara: Başbakanlık Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü Yayınları.

Berryhill, J., Bourgery T., ve Hanson A., (2018). "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", OECD Working Papers on Public Governance, No. 28, OECD Publishing, Paris, https://doi.org/10.1787/3c32c429-en.

Bouckaert, G., Peters, B.G. ve Verhoest, K. (2010), *The Coordination of Public Sector Organization: Shifting Patterns of Public Management,* Basingstoke: Palgrave Macmillan.

Burger, C., Kuhlmann, A., Richard, P. R., & Weinmann, J. (2016). Blockchain in the energy transition. A survey among decision-makers in the German energy industry. German Energy Agency, May 2020, 41. www.esmt.org

BZLab, (t.y.) BİLGEM'de Blokzincir. Erişim adresi: https://blokzincir.bilgem.tubitak.gov.tr/ bzlab.html
Christensen, T. ve Lægreid, P. (2007). The Whole-of-Government Approach to Public Sector Reform. Public Administration Review, 1060-1066.
Davidson, S., Filippi, P. D. ve Potts, J., (2016). Disrupting governance: The new institutional economics of distributed ledger technology. Erişim Adresi: https://ssrn.com/abstract=2811995
Drescher, D., (2017). Blockchain Basics: A Non-Technical Introduction in 25 steps. Apress Media LLC.
EBSI (t.y.). https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi
e-Estonia, 2016. What is e-Residency? Erişim adresi: https://e-estonia.com/solutions/e-identity/e-residency/ Erişim tarihi: 20..05.2022
E-Estonia. (t.y.). Security and safety - e-Estonia. Erişim adresi: https://e-estonia.com/solutions/security-and-safety/ Erişim tarihi: 12.02.2022.
Elisa, N., Yang, L., Li, H. ve Chao, F., (2019). Consortium blockchain for security and privacy-preserving in E-government Systems. In Proceedings of the International Conference on Electronic Business (ICEB), Newcastle Upon Tyne, UK, 8–12 December 2019; pp. 99–107.
Erdal, M. (2008). Elektronik Devlet E-Türkiye ve Kurumsal Dönüşüm. İstanbul: Filiz Kitapevi.
Erdem, E. (2014). "e-Devlet Uygulamaları Açısından Türkiye İncelemesi ve Bir Model Önerisi", Uluslararası Sosyal Araştırmalar Dergisi, 7/33, 734-746.
Eroğlu Ş., Çakmak T. ve Külcü Ö., (2015). *"Kurumlararası Bilgi Paylaşımı ve Birlikte Çalışabilirlik Esasları", e-BEYAS 2015 Sempozyumu, 21-22 Ekim 2015, Gölbaşı*
Establishing Blockchain Policy, (2019). Strategies for the governance of distributed ledger technology ecosystems. Erişim adresi: https://www.pwc.com/m1/en/publications/ establishing-blockchain-policy.html Erişim tarihi: 25.05.2022
Fang, Z., (2002). E-Government in the Digital Age: Concept, Application and Development, *International Journal of The Computer, The Internet and Management*, Vol. 10, No.2, 1-22.
Filippi, P.D., (2017), "The Interplay Between Decentralisation and Privacy: the case of Blockchain technologies", Journal of Peer Production, Alternative Internets 7
Gabison, G., (2016) "Policy Considerations for the Blockchain Technology Public and Private Applications", Bepress, European Commission
Garrett K.. (2017). Local Government in South Korea Taps Blockchain for Community Vote. Coindesk Web Site, Erişim adresi: https://www.coindesk.com/south-korea-blockchain-community-vote Erişim tarihi: 15.04.2022
Ghanem, M.E. ve Alsoufi, A., (2019). Interoperable Framework to Enhance Citizen Services in the Kingdom of Bahrain. In Proceedings of the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain. 12–14 October 2018.
Goodnow, F.J., (1983). Comparative administrative law: an analysis of the administrative systems, National and Local, of the United States, England, France, and Germany. G. P. Putnam's Sons, New York
Hellman, R. (2010). Organisational barriers to interoperability. IneChallenges, 2010 (pp. 1-9).
Hogan, M., Ojo, A., & Harney, O. (2017). Public Administration and Information Technology.

Huynh, T. T., Nguyen T. D. ve Tan H., (2019). “A Survey on Security and Privacy Issues of Blockchain Technology.” In: *2019 International Conference on System Science and Engineering (ICSSE)*. Dong Hoi, Vietnam, 362–367.

Iansiti, M. ve Lakhani, K. R. (2017). The Truth About Blockchain. Harvard Business Review. https://hbr.org/2017/01/the-truth-about-blockchain

International Telecommunication Union, (2008). Electronic Government for Developing Countries, https://www.itu.int/ITU-D/cyb/app/docs/e-gov_for_dev_countries-report.pdf

Intersessional panel of the United Nations Commission on science and technology for development (CSTD): Contribution by Contribution by Turkey to the CSTD 2020-2021 priority theme on “Harnessing blockchain for sustainable development: prospects and challenges” (2020). Geneva, 5. Erişim adresi: https://unctad.org/system/files/non-official-document/CSTD_2020-21_c33_B_Turkey_en.pdf

İntepe, A. S. (2020). Güncel Gelişmeler Işığında Kamu Yönetiminde Kurumlar Arası Koordinasyon. Türk İdare Dergisi, (490), 141-164.

Jae-yeon, W. (2020). NH Nonghyup, Kore’nin ilk dağıtılmış kimlik uygulamasını ’mobil çalışan kimliği’ni tanıttı. Erişim adresi: https://news.joins.com/article/23714789 Erişim tarihi: 01.04.2022

Karagülmez, A. (2010). “Elektronik Devlet Kavramı”. Türkiye Adalet Akademisi Dergisi, (2), 449-476.

Karakaya, Z., Akkaş, A., Ersun, F. L., Yılmazer, M., Özdemir, Ö., ve Öztürk, Ö. (2004). e-Devlet: Kamuda Ortak Bilgi-Veri Paylaşımı 2. Ara Rapor. TBD, Ankara, Mart.

Kassen, M. (2021). Blockchain and e-government innovation: Automation of public information processes. Information Systems, 101862. https://doi.org/10.1016/j.is.2021.101862

Kırçova, İ. (2003). E-Devlet Uygulamaları ve Ekonomiye Etkileri. İstanbul Ticaret Odası: Acar Matbaacılık.

Kıymık, Z. (2019). Blokzincir teknolojisinin kredi transferinde kullanımı (Yükseklisans tezi). Erişim Adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Klischewski, R. Ve Scholl, H. J. (2006). Information quality as a common ground for key players in e- government integration and interoperability. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on, 4*, (pp. 72-72).

Korea Plans to Adopt Blockchain in Seven Sectors with a Goal to Promote Decentralized Identifiers. (2020). Erişim adresi: https://www.msit.go.kr/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=441 Erişim tarihi: 15.04.2022

Lindman, J., v.d. (2020), "The uncertain promise of blockchain for government", OECD Working Papers on Public Governance, No. 43, OECD Publishing, Paris, https://doi.org/10.1787/d031cd67-en.

Liu, L., Piao, C., Jiang, X. ve Zheng, L. (2018). Research on Governmental Data Sharing Based on Local Differential Privacy Approach. In Proceedings of the 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), Xi’an, China, 12–14 October 2018; pp. 39–45.

Malavolta G., Moreno-Sanchez P., Kate A., Maffei M. and Ravi S., (2017) "Concurrency and Privacy with Payment Channel Networks", *CCS*, pp. 455-471.

Martindale, J., (2018). What is a blockchain? Here's everything you need to know. Digital Trends. Computing. Erişim Adresi: https://www.digitaltrends.com/computing/what-is- a-blockchain/

Mattila, J., (2016). *The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures*. The Research Institute of the Finnish Economy. https://ideas.repec.org/p/rif/wpaper/38.html

Melitski, J., Carrizales, T. J., Manoharan, A., ve Holzer, M. (2011). Digital Governance Success Factors And Barriers To Success Prague. *International Journal of Organization Theory and Behavior, 14*(4), 451- 472.

Mergel, I., Schweik, C. M. ve Fountain, J. E. (2009). "The Transformational Effect of Web 2.0 Technologies on Government", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1412796

Mougayar, W., (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons, Incorporated.

Naing, T.T., (2019). Initiation of Blockchain Technology based Open Framework for e-Government Development in Myanmar. In Proceedings of the Myanmar Universities' Research Conference (MURC 2019), Yangon, Myanmar, 24-25 June 2019; pp. 1–7.

Nakamoto, S., (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://nakamotoinstitute.org/bitcoin/

OECD Blockchain Primer, (2018). Erişim Adresi: http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

OECD STI Scoreboard.(2021). https://www.oecd.org/sti/scoreboard.htm.DOI: 10.30783/nevsosbilen.748379

Özaltın, O. ve Ersoy, M. (2020). Kamu Yönetiminde Blokzincir Kullanımı: D5 Örneği. Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, 10(2), 746-763.

Paul, A. ve Paul, V. (2012). The e-Government interoperability through Enterprise Architecture in Indian perspective. In *Information and Communication Technologies (WICT), 2012 World Congress on,* (pp. 645-650).

Petter, S., DeLone, W., ve McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European journal of information systems, 17*(3), 236-263.

Politou, E., Casino, F., Alepis, E. ve Patsakis, C. (2019). Blockchain Mutability : Challenges and Proposed Solutions. IEEE Transactions on Emerging Topics in Computing, April 2020. https://doi.org/10.1109/TETC.2019.2949510

Priit M. (2018). Estonia – the Digital Republic Secured by Blockchain. Estonia: PWC.

Rikken, O., Janssen, M., ve Kwee, Z., (2019). Governance challenges of blockchain and decentralized autonomous organizations. Information Polity, 24(4), 397–417. https://doi.org/10.3233/ip-190154

Roman, A.V., (2013). Realizing E-government: delineating implementation challenges and defining success. In: Halpin E.F., Griffin D., Rankin C. et al Digital public administration and E-government in developing nations: policy and practice. IGI Global, Pennsylvania, p.112

Seferoğlu, S. S., Çelen, F. K. ve Çelik, A., (2011). Bölüm 19 Türkiye'de E-Devlet Uygulamaları: Sorunlar ve Çözüm Önerileri Üstüne Bir Analiz. *Türkiye'de E-Öğrenme: Gelişmeler ve Uygulamalar-II*, 281.

Shen, M., Zhu, L., ve Xu, K. (2020). Blockchain: empowering secure data sharing (pp. 1-130). Singapore: Springer. Erişim Adresi: https://link.springer.com/book/10.1007%2F978-981-15-5939-6

Sobacı M.Z. (2012), "e-Devlet: Kuramsal Bir Bakış", e-Devlet Kamu Yönetimi ve Teknoloji İlişkisinde Güncel Gelişmeler, ed. Mehmet Zahid Sobacı-Mete Yıldız, Nobel Yayıncılık, Ankara, s.8

Sohimi, M. B., ve Abbas, W. F. B. (2011). The prioritization factors of Enterprise Application Integration (EAI) adoption in Malaysian e-Government. In *Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on* (pp. 1-6).

Solli-Sæther, H. (2010). Analytical framework for e-government interoperability. In *eChallenges, 2010* (pp. 1- 9).

Stemberger, M. I., & Jaklic, J. (2007). Towards E-government by business process change—A methodology for public sector. *International Journal of Information Management, 27*(4), 221-232.

T.C. Başbakanlık (2009). Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları, 2009/4 Sayılı Başbakanlık Genelgesi.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (t.y.). Dijital Türkiye Projesi. Erişim Adresi: https://cbddo.gov.tr/projeler/dijital-turkiye-v1.0/

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, (2019). Türkiye Cumhuriyeti 11. Kalkınma Planı (2019-2023). http://www.sbb.gov.tr/wp-content/uploads/2019/07/ OnbirinciKalkinmaPlani.pdf

T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi, (2012). e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.1. Erişim adresi: http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Birlikte_Calisabilirlik_ Esaslari_Rehberi_2.1.pdf

T.C. Sanayi ve Teknoloji Bakanlığı, (2019). 2020-2024 Stratejik Planı.

T.C. Ulaştırma ve Altyapı Bakanlığı Bakanlığı, (t.y.), KamuNet, Erişim adresi: https://hgm.uab.gov.tr/kamu-net

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, (2015), 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı.

Torres, L., Pina, V. ve Royo, S. (2005), "E-Government and the Transformation of Public Administrations in EU Countries: Beyond NPM or just a Second Wave of Reforms?", Online Information Review, Vol.29, No.5, ss.531-553.

Turkey to the CSTD 2020-2021 priority theme on "Harnessing blockchain for sustainable development: prospects and challenges" (2020). Geneva, 5. Erişim adresi: https://unctad.org/system/files/non-official-document/CSTD_202021_c33_B_Turkey _en.pdf

UN E-Government Knowledgebase. United Nations. (2021). https://publicadministration. un.org/egovkb/en-us/Data-Center.

Usta, A. ve Doğantekin, S., (2019). Blockchain 101 v2, Erişim Adresi: https://bit.ly/Blockchain101_v2_r2.

Wessling F., Ehmke C., Hesenius M. ve Gruhn V., (2018). How much blockchain do you need? Towards a concept for building hybrid DApp architectures. In: Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain. Association for Computing Machinery, Gothenburg, pp 44–47

Wong, P. F., Chia, F. C., Kiu, M. S., ve Lou, E. C. W. (2020). Potential integration of blockchain technology into smart sustainable city (SSC) developments: a systematic review. Smart and Sustainable Built Environment. https://doi.org/10.1108/SASBE-09-2020-0140

Wüst K. ve Gervais A ., (2018). Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). CPS. IEEE, Piscataway, pp 45–54

Xu X., Weber I. ve Staples M., (2019). Architecture for blockchain applications. Springer International Publishing, Cham

Yaga, D., Mell, P., Roby, N. ve Scarfone, K., (2018). "Blockchain Technology Overview", United States National Institute of Standards and Technology (NIST), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202- draft.pdf

Yano M., Dai C., Masuda K. ve Kishimoto Y., (2019). Creation of a blockchain and a new ecosystem. RIETI policy discussion papers

Yıldırım, M. (2010). Kamu yönetimine güven: e-devlet açısından bir inceleme. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *11*(1), 1-19.

Young, J. (2019). Here's how the gov't of Seoul is using a public blockchain in the real-world. CCN.com. Erişim adresi: https://www.ccn.com/heres- how-the-govt-of-seoul-is-using-a-public-blockchain-in-the-real-world/. Erişim tarihi: 20.05.2022

Young-sil, Y. (2018). Korean gov't Unveils blockchain technology development strategy. Businesskorea. Erişim adresi: http://www.businesskorea.co.kr/news/articleView.html?idxno=23184. Erişim tarihi: 15.04.2022

Zhang, Y., Deng, S., Zhang, Y. ve Kong J., (2019). Research on Government Information Sharing Model Using Blockchain Technology. In Proceedings of the 10th International Conference on Information Technology in Medicine and Education (ITME), Qingdao, China, 23–25 August 2019; pp. 726–729.

Zheng, BK., Zhu, LH., Shen, M., v.d. (2018). Scalable and Privacy-Preserving Data Sharing Based on Blockchain. *J. Comput. Sci. Technol.* 33, 557–567.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : SAYIN, Mustafa

Uyruğu : T.C.

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek lisans	Ankara Hacı Bayram Veli Üniversitesi	2022
Lisans	Anadolu Üniversitesi İşletme Fakültesi	2007
Lise	Çok Programlı Astsubay Hazırlama Okulu	2002


ankara
HBM