IJEASED

INTERNATIONAL JOURNAL OF EASTERN ANATOLIA SCIENCE ENGINEERING AND DESIGN

Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi
ISSN: 2667-8764 , 1(2), 260-295 , 2019
https://dergipark.org.tr/tr/pub/ijeased

Araştırma Makalesi / *Research Article*

Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları

Mustafa TAKAOĞLU [1*], Çağdaş ÖZER [2], Emre PARLAK [3]

[1] İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, 34295, Türkiye
[2] İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, İstanbul, 34295, Türkiye
[3] İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Elektrik Elektronik Müh. Bölümü, İstanbul, 34295, Türkiye

Yazar Kimliği / *Author ID (ORCID Number)*	Makale Süreci / *Article Process*	
[*]**Sorumlu Yazar** / *Corresponding author* : mustafatakaoglu@aydin.edu.tr	**Geliş Tarihi** / ***Received Date*** :	06.11.2019
https://orcid.org/0000-0002-1634-2705, M. Takaoğlu	**Revizyon Tarihi** / ***Revision Date*** :	26.11.2019
https://orcid.org/0000-0002-0581-7955, Ç. Özer	**Kabul Tarihi** / ***Accepted Date*** :	10.12.2019
https://orcid.org/0000-0003-2668-1660, E. Parlak	**Yayım Tarihi** / ***Published Date*** :	15.12.2019

Alıntı / ***Cite*** **:** Takaoğlu, M., Özer, Ç., Parlak, E. (2019). Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları, Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi, 1(2), 260-295.

Özet

Kripto paraların elde ettiği başarı sonrası dikkatleri üzerine çekmeyi başaran blokzincir teknolojisi, gelişmekte olan ve popüler bir çalışma konusudur. Merkeziyetçi olmayan yapısı, tek yönlü ve silinemez veri kaydı, şifrelenmiş blok mimarisi ve üçüncü şahıslarca kurcalanmaya müsaade etmeyen veri yapısıyla birçok soruna çözüm olacak niteliktedir. Destekleyici bir teknoloji olan blokzinciri, birçok farklı teknolojiye entegre edilmeye çalışılmaktadır. Bu sebeple makalemizde blokzincir teknolojisinin hangi alanlarda kullanıldığı ve ne gibi sonuçlar elde edildiği araştırılmıştır. Blokzincir teknolojisinin sağladığı avantajlar ve karşılaştığı zorluklar hakkında elde edilen bilgiler paylaşılmıştır. Yapmış olduğumuz araştırmalar sonucunda blokzincir teknolojisinin Türkiye'de hangi alanlarda uygulanabileceği belirlenmiştir. Blokzincir teknolojisinin uygulama alanları olarak bankacılık uygulamaları, internet güvenliği, tedarik zinciri, nesnelerin interneti, sigortacılık, kişisel ve toplu ulaşım, online veri saklama, vakıf ve bağış işlemleri, oy verme süreçleri, kamu uygulamaları, sağlık uygulamaları, enerji yönetimi, fikri mülkiyet ve telif hakkı uygulamaları, emlak ve tapu uygulamaları, dijital kimlik, akıllı şehirler, akıllı sözleşmeler ve hukuki uygunluklarının incelenmesi, eğitim alanında uygulamaları gibi on sekiz farklı çalışma konusu tespit edilmiş ve edinilen bilgiler paylaşılmıştır.

Anahtar Kelimeler: Blokzincir Teknolojisi, Akıllı Sözleşmeler, Nesnelerin İnterneti, Akıllı Şehirler, Dağıtık Veri Yapıları.

Blockchain Technology and Possible Implementation Areas in Turkey

Abstract

Blockchain technology, which succeeds in attracting attention after the success of cryptocurrency, is a developing and popular subject of study. With its decentralized structure, decentralized and indelible data recording, encrypted block architecture, and data structure that does not allow tampering by third parties, it is capable of solving many problems. Blockchain, a supporting technology, is being tried to be integrated into many different technologies. For this reason, in this article, in which areas blockchain technology is used and what results are obtained were shared. Information about the advantages and challenges of blockchain technology is shared. As a result of the researches we have done, it has been determined which study areas blockchain technologies can be applied in Turkey. As the application areas of blockchain technology, banking applications, internet security, supply chain, internet of objects, insurance, personal and public transportation, online data storage, foundation and donation processes, voting processes, public applications, health applications, energy management, intellectual property and copyright rights applications, real estate and title deed applications, digital identity, smart cities, smart contracts and legal compliance examination, applications in the field of education were identified and the information obtained was shared.

Keywords: *Blockchain Technology, Smart Contracts, Internet of Things, Smart Cities, Distributed Data Structures.*

1. Giriş

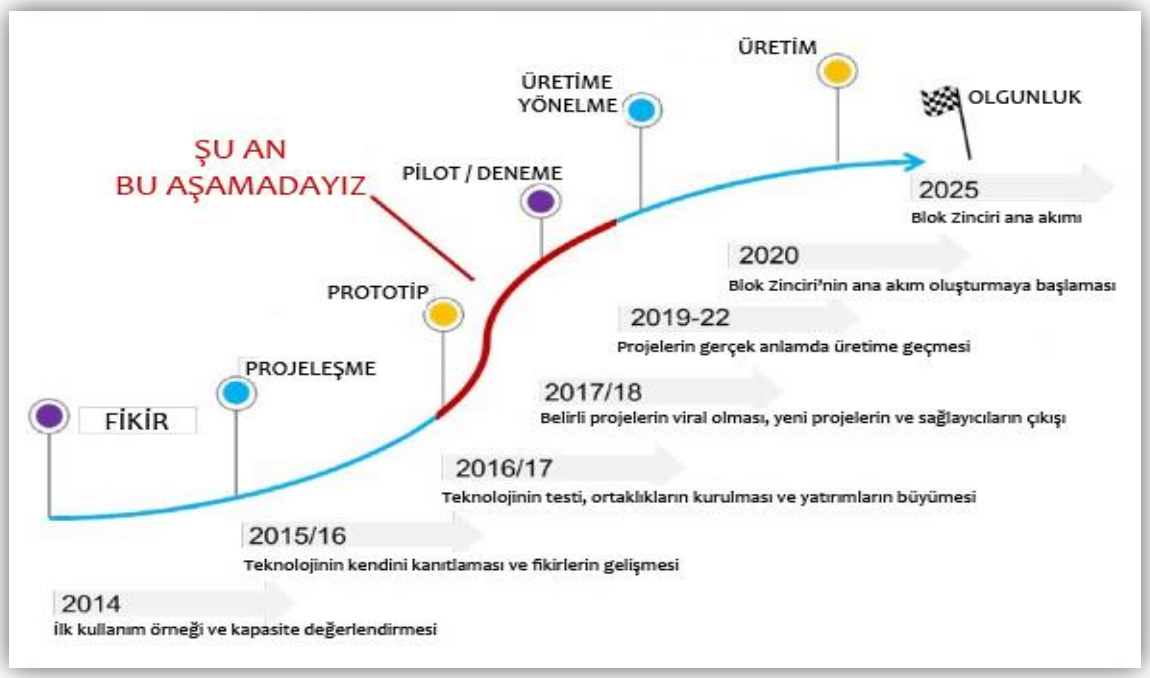
Blokzincir teknolojisi günümüzde birçok alanda uygulanmaya çalışılan popüler bir konu olsa da yeni önerilmiş bir çalışma konusu değildir. Blokzincir mimarisi, 1991 yılında Stuart Haber ve W. Scott Stornetta adlı kriptograflar tarafından, spesifik bir sorunun çözümü için önerilmiş ve elde edilen sonuçlar paylaşılmıştır (Takaoğlu ve ark., 2018). Ancak tarihsel bir açıdan baktığımızda teknolojinin köklerinin Ralph C. Merkle'nin 1970'lerin sonunda Merkle ağacını önerdiğinde karşımıza çıktığı görülmektedir. Merkle ağacında dijital imzalar için bir ağaç yapısında birleştirilmiş özütleme algoritmalarının kullanılmasını önermiştir. Özütleme algoritmaları ise 1950'lerden beri bilgi güvenliği, dijital imzalar ve mesaj bütünlüğü doğrulaması için kriptografide yaygın olarak kullanılan algoritmalardır. Merkle fikrinden yaklaşık on yıl sonra, Leslie Lamport güvenli giriş için bir karma zincir kullanmayı önermiştir. 1990'da elektronik ödemeler için ilk şifreleme parası olan e-Cash tanımlanmıştır. Karma zincir konseptinin daha da evrimleşmesi ve iyileştirmeleri 1994 tarihli yazıda, Neil Haller tarafından Unix oturum açma için bir karma zincir olan S / KEY ile tanıtılmıştır. 2002'de, Adam Back, blokzinciri temelli bir elektronik para birimi olan ve Bitcoin'in özelliklerinin çoğuna sahip olan bir işin ispatı uzlaşma algoritmasıyla çalışan hashcash'ı önermiş ve Satoshi Nakamoto tarafından Bitcoin'in referans çalışması olarak gösterilmiştir (Aste ve ark., 2017).

Günümüzde bu kadar ilgi çekici hale gelmesinin sebebi yukarıda da belirtildiği üzere 2008 yılında Satoshi Nakamoto mahlaslı, kim olduğu bilinmeyen kişi ya da kişiler tarafından önerilen Bitcoin kripto parası sayesinde olmuştur (Nakamoto, 2008). Bitcoin kripto parası, blokzincir temelleri üzerinde oluşturulmuş (Nadiya ve ark., 2018), dolayısıyla kriptoloji biliminin sistemin

güvenliğini sağladığı, arada üçüncü şahısların bulunmadığı bir ödeme sistemi olarak karşımıza çıkmaktadır. Bitcoin kripto parasının ortaya çıkmasını gerektirecek ortamı irdelemek gerekirse, 2008 yılında patlak veren Amerikan merkezli krizde, Mortgage taşınmaz kredileri ile ilgili bilgileri paylaşan merkezi otoritelerin gerçekçi olmayan veriler ışığında işlemler yapması sebebiyle ortaya çıkmış bir krizdir. Bu kriz ortamında, merkezi otoritelerin insanlara vermiş olduğu güvensizlik sebebiyle bir tepki olarak doğan Bitcoin, merkezi otoriteyi saf dışı bırakarak, işlemlerin karşılıklı olarak yapılmasını önermiş ve ortaya bir mimari koymuştur. Bitcoin kripto parasının maddi değerinin aşırı miktarlarda artması, sahip olduğu voladitenin yüksekliğine rağmen insanların ilgisini çekmiş ve günümüzde gelinen süreçte Bitcoin ve Bitcoinden sonra üretilen tüm kripto paralara verilen ad olan Altcoinlere olan ilgi artarak devam etmiştir.

Blokzincir teknolojisinin bu kadar popüler olmasına katkı sağlayan Bitcoin, anlaşılabilir bir şekilde insanların algısında blokzincir denilince direkt Bitcoin düşünülmesine neden olmaktadır. Ancak bu bakış açısı doğru bir yaklaşım değildir. Bitcoin, blokzincir teknolojisinin çalışma konularında sadece birisidir. Blokzincir teknolojisi için karşılaşılan tüm problemlere mucizevi bir şekilde çözüm sağlayacağı algısı da doğru değildir. Çünkü blokzincir teknolojisi destekleyici bir teknolojidir. Yani hali hazırda bulunan çalışma konularının desteklenmesi noktasında faydalar sağlar. Örneğin çalışmamızın ilerleyen bölümlerinde açıklanan blokzinciri mimarisinin sağlamış olduğu katkılar sayesinde, günümüzde kullanılan birçok veri merkezinin sahip olduğu merkezi yapısı sebebiyle karşılaşılan güvenlik sorunlarına bir çözüm önermeyi başarmıştır.

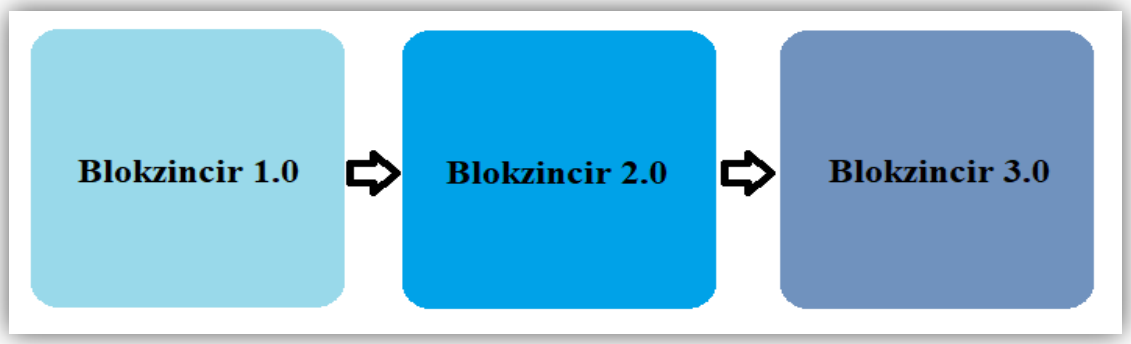
İnternet teknolojisinin gelişimi ile blokzincirinin gelişimi için bir benzetilme durumu söz konusudur. İnternet teknolojisinin 90'lı yıllarda ortaya çıkmasından günümüze kadar gelen süreçte görülen gelişim düşünüldüğünde blokzincirinin de benzer bir gelişme kaydedeceği fikri iyimser ancak gerçekçi bir bakış açısıdır. Aşağıdaki Şekil 1'de blokzinciri teknolojisinin gelişim süreçleri ile ilgili bir görsel paylaşılmıştır. Buradan anlaşılacağı üzere, günümüzde yapılan çalışmalar blokzincir teknolojisi ile geliştirilmiş prototiplerin üretilmesi ve denemelerinin yapılması aşamasındadır. Bu noktada ülkemizde yapılan birçok araştırma olup, blokzinciri teknolojisi özelinde düşünüldüğünde kaçırılmış yahut ardında kalınmış bir gelişme bulunmamaktadır. Ayrıca blokzincir çalışma alanı çokça yatırım alan bir çalışma konusudur. Günümüzde 1500'den fazla altcoin bulunmakta ve 480 milyar dolardan fazla bir pazar payına sahiptir (Lee, 2018). İlerleyen süreçte kripto paralar hariç tutularak düşünüldüğünde blokzinciri teknolojisinin yüz milyarlarca dolarlık bir büyüklüğe ulaşması beklenen bir gelişmedir.



Şekil 1. Blokzincir teknolojisi gelişim aşamaları (Miraz ve Ali, 2018)

1.1. Blokzincir Gelişim Evreleri

Satoshi'nin 2008 yılında önerdiği blokzinciri uygulaması finansal bir çözüm önermiştir. Blokzincirinin bu aşamasına Blokzincir 1.0 denmektedir. Nick Szabo tarafından 1994 yılında ortaya atılan akıllı sözleşme fikri, Solidity programlama dili yardımıyla Ethereum tabanlı olarak uygulanılmıştır (Szabo, 1994). Akıllı sözleşmelerin çalışıldığı bu aşamaya Blokzincir 2.0 denilmektedir. Blokzincir teknolojisinin uygulanma alanlarının genişliğinin fark edilmesi ve bu alanda yapılan çalışmalar sonucunda teknolojinin finans ve akıllı sözleşmeler dışındaki alanlarda uygulanması aşamasına da Blokzincir 3.0 denilmektedir. Günümüzde Blokzincir 4.0 için çeşitli açıklamalar yapılmaktadır. Yapay zeka algoritmaları ve blokzincir teknolojisinin hibrit edilerek elde edilebilecek sonuçlar için Blokzincir 4.0 denileceği düşünülmektedir. Ancak günümüzde bu noktada kabul görmüş bir tanım ileri sürmek pek mümkün değildir. Şekil 2'de açıkladığımız gelişimle ilgili bir görsel paylaşılmıştır.



Şekil 2. Blokzincir gelişim adımları

Araştırmamızda blokzincir teknolojisinin uygulama alanlarının neler olduğu ve ülkemizde hangi alanlarda uyarlanabileceği üzerine çalışılmıştır. Paylaşılan bilgilerin daha iyi anlaşılması amacıyla blokzincir teknolojisinin teknik açıklamalarına yer verilmiştir. Teknolojinin avantaj ve dezavantajları hakkında edinilen bilgiler paylaşılmıştır.

2. Blokzincir Teknolojisi

Blokzinciri teknolojisi, eşler arası ağ ilkeleri, asimetrik şifreleme ve dijital imza gibi kriptografik ilkeler altında oluşturulmuş dağıtık bir mimaridir (Balaskas ve Franqueira, 2018). Blokzinciri, tamper-proof yani kurcalamaya karşı korumalı dijital işlem defteri oluşturur ve defteri paylaşır, böylece şeffaflık sağlanmış olur (Kshetri ve Voas, 2018). Aynı zamanda değiştirilemeyen veriler sistemlerin güvenliğin daha güçlü olmasını sağlar. Bu sebeple blokzinciri için bir ağ üzerinde çalışan bir fikir birliği algoritması tarafından yönetilen dağıtılmış ve değişmez bir veri yapısıdır tanımı yapılabilir (Duan ve ark., 2019).

Şekil 3. Blokzincir küresel bir dağıtık defter mimarisidir (Nishith Desai Associates, 2016)

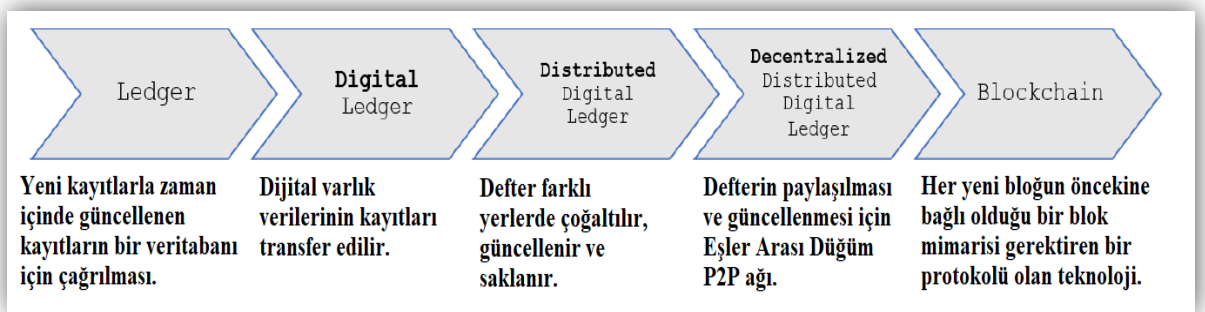
Blokzinciri teknolojisi için kullanılan dağıtık defter mimarisi (Lou ve ark., 2018) tanımı çok isabetli bir açıklamadır. Çünkü teoride sistemin çalışması aynı bir defterin sayfaları gibi işler. Her bir sayfa kullanıcılar tarafından doldurulur. Doldurulan sayfadan sonra bir sonraki sayfaya geçilir ve doldurulan tüm bilgiler defterin önceki sayfalarında bulunmaya devam eder. Geleneksel defterlerden farklı olarak blokzincirinde her bir sayfa bir sonraki sayfaya kriptolojik bir özütleme algoritmasıyla bağlanır ve deftere veri girilme yönü hep tek taraflıdır. Blokzincirinde özütleme işlemi Şekil 4'te paylaşılmıştır. Ayrıca Şekil 5'de bir özütleme algoritması olan SHA 256 (Secure Hashing Algorithm 256) isimli özütleme algoritmasının çalışma mantığına dair bir örnek paylaşılmıştır.

Şekil 4. Özütleme fonksiyonu (Singh ve ark., 2018)

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

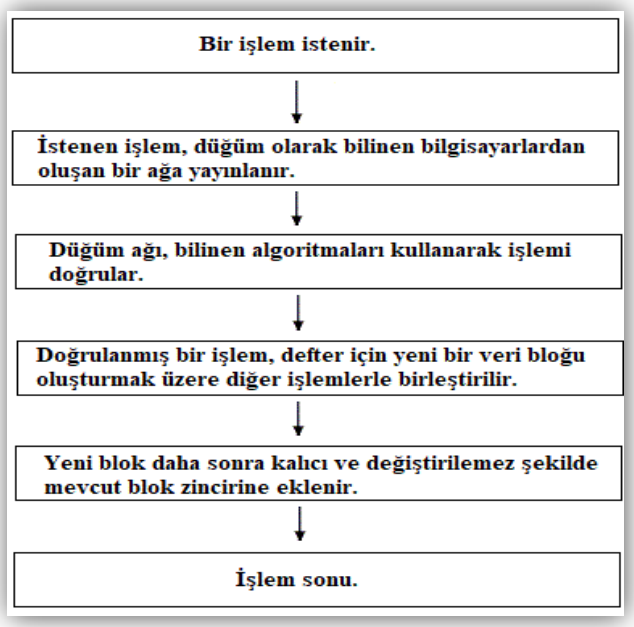
Şekil 5. Özütleme algoritması SHA 256 (Mitra, 2019)

Blokzincirlerine yazılan bir bilgi geri alınamaz yahut değiştirilemez. Bu durumda akıllarda canlanan ilk soru yanlış girilen bilgilerin durumudur. Veri girişinin insanlar nezdinde yapıldığı tüm uygulamalarda hata olabilir. Bu durumda blokzinciri kullanılarak geliştirilmiş bir veri merkezinde düzeltme işlemi şu şekilde olacaktır: Yazılmış olan veri olduğu gibi kalacak ve yeni girilecek düzeltme verisi de sistemde gözükecektir. Yani hem hatalı veri hem de düzeltilmiş hali sistemde gözükecektir. Bu tarz bir mekanizmanın olması dahi şeffaflık açısından birçok problemin çözümü olacak niteliktedir. Şekil 6'de geleneksel defter yapısından dağıtık defter mimarisine geçişin aşamaları paylaşılmıştır.



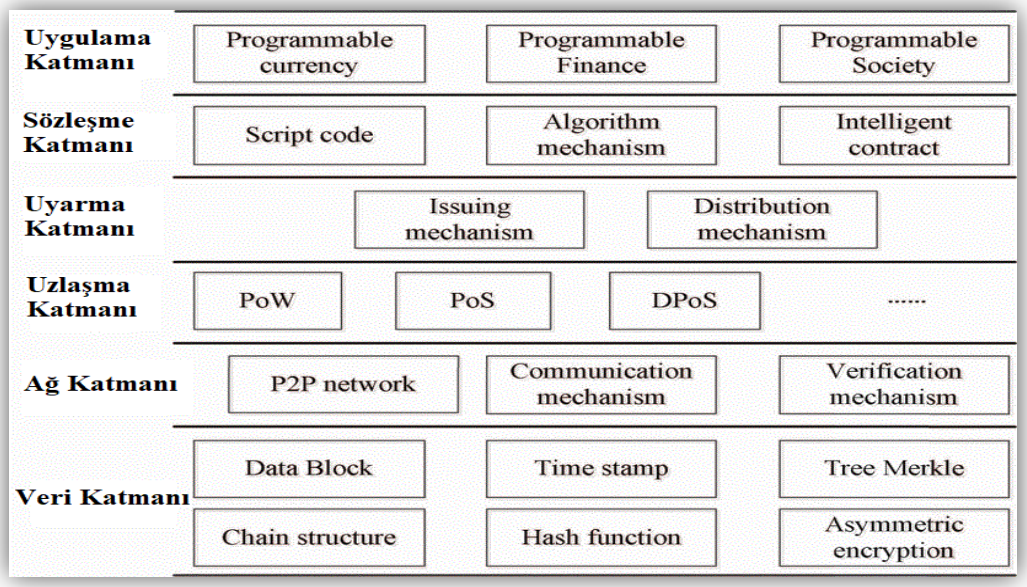
Şekil 6. Geleneksel defter mimarisinden blokzincirine geçiş (Belotti ve ark., 2019)

Oluşturulan bir blokzincir sisteminde, bir işlemin oluşturulmasından sonlandırılmasına varıncaya kadar geçen süreçte izlenen adımlar Şekil 7'te paylaşılmıştır. Blokzincirleri sisteme erişim izni verilen kullanıcılara göre çeşitlendirilmektedir. Bitcoin gibi tüm kullanıcıların erişimine müsaade edildiği sistemlere genel (public) blokzincir denilmektedir. Bitcoin dünyadaki en büyük genel blokzincir örneğidir (Kolekar ve ark., 2018). Bir diğer blokzinciri türü özel (private) blokzinciridir. Özel blokzincirde okuma, yazma ve uzlaşma işlemlerine erişebilecek kullanıcılar önceden belirlenmiştir. Gerektiğinde zincirdeki düğümler eklenir veya çıkarılır. Özel blokzincirlerinde bu özellik sayesinde kötü amaçlı düğümlerin ağa girmesi mümkün değildir. PoW (Proof of Work) gibi işlemler olmadan yeterli güvenlik sağlanır (Kang ve ark., 2018). Konsorsiyum blokzincirinde ise karar verici düğümler belirlenmiştir. Bu düğümler blok doğrulama işlemlerini gerçekleştirirler ve sisteme erişebilecek düğümlere de karar verirler. Konsorsiyum blokzincirlerinde verimlilik ve güvenlik yüksektir. Son olarak günümüzde hibrit blokzincir çalışmaları da yapılmaktadır. Bu tarz blokzincirlerinde sistem oluşturulurken saklanacak verilerin seçilmiş bir kısmı blokzincirinde tutulur ve blokzincirinde saklanmayan kısmı geleneksel yöntemlerle işlenebilmektedir (Ra ve Lee, 2019).



Şekil 7. Blokzincir çalışma mekanizması (Bhat ve Vijayal, 2017)

Blokzinciri sistemlerini yapısal olarak incelediğimizde katmanlı bir yaklaşımda bulunarak altı katmandan bahsedebiliriz. Bunlar; uygulama katmanı, sözleşme katmanı, uyarlama katmanı, uzlaşma katmanı, ağ katmanı ve veri katmanıdır. Paylaşılan blokzincir katmanlarının alt içerikleri Şekil 8'de paylaşılmıştır.



Şekil 8. Blokzincir sisteminin yapısı (Liu ve Li, 2018)

Özellikle üzerinde durulması gereken katmanlardan birisi uzlaşma katmanıdır. Bu katmanda bir blokzincirinin kullandığı uzlaşma algoritması seçilidir. Her uzlaşma algoritmasının bir özelliği bulunmaktadır. Kurulacak sistemin özellikleriyle seçilecek uzlaşma algoritmasının uygunluğu büyük önem arz etmektedir. Doğal olarak başarılı bir blokzincir sistemi tasarlamak ve hayata geçirmek için tecrübeli yazılımcılar ve bilgisayar bilimcileri ile çalışmak gerekmektedir. İyi oluşturulmuş bir ekip tarafından gelecekte karşılaşılacak kullanıcı hacmi ve veri yükü gibi değişkenlerin tutarlı optimasyonunun yapılması büyük öneme sahiptir. Literatürde çokça kullanılan uzlaşma algoritmaları; PBFT, Stellar, Ripple, Proof of Work (PoW), Proof of Stake (PoS), Threshold Relay, Proof of Authority (PoA), Proof of Burn (PoB), Proof of Elapsed Time (PoET) gibi algoritmalardır (Dinh ve ark., 2018).

PoW ve PoS gibi uzlaşma algoritmalarının kullanıldığı blokzinciri sistemlerine yapılan belli başlı saldırılar bulunmaktadır. Bunlar; %51 saldırısı, çift harcama saldırısı, Sybil saldırısı, DDos saldırısı ve Shora gibi kuantum algoritmaları kullanarak sistemin kullandığı kriptografik şifrelemelerin kırılması saldırılarıdır (Golosova ve Romanovs, 2018). Bu saldırıların başarı oranı çok düşük olmakla birlikte başarılı sonuç elde etme ihtimali de bulunmaktadır. Gelişen özütleme algoritmaları, uzlaşma protokolleri ve kuantum hesaplama teknolojisinin uygulama olanaklarının artması ile birlikte geliştirilecek blokzincir sistemlerinin güvenlik açısından hali hazırdaki seviyeden çok daha kuvvetli bir hale gelmesi beklenmektedir.

Son olarak akıllı sözleşmelerden bahsetmek gerekmektedir. Akıllı sözleşmeler blokzincirlerinde dinamik işlerin yapıldığı kısımlar olarak düşünülebilir. Adından da anlaşılacağı üzere akıllı sözleşmeler yazılımsal olarak hazırlanmış dijital birer sözleşmedir. Özel bir durumun çözümü için geliştirilen bu sözleşmeler blokzincir sisteminde bir kod olarak karşımıza çıkmaktadır. Sadece geliştirildiği durum ile karşılaşıldığı zaman çalışan bu sistemler kodlandıktan sonra düzeltme yapılamadığı için çok dikkatli optimize edilmeleri gerekmektedir (Tanrıverdi ve ark., 2019).

2.1. Blokzinciri Teknolojisinin Avantaj ve Dezavantajları

Blokzinciri teknolojisinin kullanımının sağlamış olduğu avantajlar bulunmaktadır. Blokzincirinin dağıtık bir yapıya sahip olması sayesinde veriler merkezi bir sunucuda saklanmadığı için teknik arızalara ve siber saldırılara karşı koruma sağlamaktadır. Siber saldırıların engellenmesi doğrudan dolandırıcılık girişimlerinin düşürülmesini sağlamaktadır.

Blokzincirinde işlemlerin tek yönlü olması, tüm düğümler tarafından onaylanmış bir işlemin değiştirilemez olması ve tüm değişikliklerin erişim hakkı olan düğümler tarafından şeffafça izlenebilir olması sebebiyle sistemde bir istikrar sağlanmaktadır.

Kripto paraların kullanımının artması, eşler arası iletişim özelliği sayesinde aradan üçüncü kurum ya da kuruluşları çıkararak maliyetleri azaltma imkânı sağlamıştır. Ayrıca finans kuruluşlarının kriz durumlarında anlaşılan gerçek dışı bilgi paylaşımları, müşterilerine yansıtılan gizli ücretlendirmeler blokzinciri teknolojisinin finans uygulamalarında kullanımının artması durumunda şeffaflığı arttıracağı için kurumlara duyulan güvenilirliğin artmasını ve müşterilerin bilgisi dışında yansıtılan en küçük bir ücretin dahi herkesçe bilinmesini sağlayacaktır. Ayrıca Bitcoin ve Ethereum başta olmak üzere tüm kripto paralar için güvencesiz yani devlet kurumlarınca güvence verilmeyen sistemler olmaları eleştirisi blokzinciri teknolojisinden ayrı bir meseledir. Günümüzde birçok devlet kurumları blokzincirinin finans uygulamaları üzerine çalışmalar yürütmektedir. Dubai (Emcash), Venezuela (Petro), Estonya (Estcoin), Rusya (Crypytoruble), İsveç (E-Krona), Japonya (J-coin) gibi ülkeler kendi kripto parasını üretmiş, diğer birçok ülke de bu alanda çalışmalarına devam etmektedir. Devletlerin üretmiş oldukları bu kripto paralar yine devlet güvencesi altında insanların kullanımına sunulacak paralar olacaktır.

Blokzinciri sistemleri her sorunu çözen bir teknoloji değildir. Teknolojinin gelişim aşamasında olması ve yeni uygulama alanlarıyla birlikte fark edilen yeni sorunlar giderilmeye çalışılmaktadır. Örneğin Bitcoin kripto parasının kullanımının çok yüksek olması sayesinde birçok eksiklik göze çarpmıştır. Bunların en başında ölçeklenebilirlik gelmektedir (Saltykov ve Rusyaeva, 2018). Bitcoin blokzinciri platformu saniyede 4 işlem yapabilirken, Ethereum blokzincir platformu saniyede 12 işlem yapabilmektedir. Bu işlem gücü Visa kart sistemi ya da en basitinden Facebook'un saniyede yaptıkları işlem kapasitesi ile karşılaştırıldığında kabul edilemez bir seviyededir(Salah ve ark., 2019).

Uzlaşma algoritmaları üzerinde çokça çalışılan bir konu olmasına rağmen halen kullanılan uzlaşma algoritmalarının zayıf yönleri devam etmektedir. Örneğin PoW algoritması madencilik işlemlerinde verimsiz, PoS algoritması ise işlem onaylama aşamasında yeteri kadar performanslı çalışmamaktadır (Ma ve ark., 2018).

Bilindiği üzere blokzincir sistemleri zaman geçtikçe büyümekte ve veri saklanması açısından alternatif çözümler bulunmalıdır. Günümüzde bir blokzinciri sistemi ortalama 200 GB'lık bir depolama alanına ihtiyaç duymaktadır. Bilgisayarlardaki sabit disklerin boyutları ile kurulan

blokzincir sistemlerinin zamanla gereksinim duyacağı depolama alanı arasında uyumsuzluk bir sorun haline gelebilmektedir.

Bir diğer sorun da blokzincirlerinin kriptolojik bir ürün olmaları sebebiyle kullandıkları "private key" denilen özel anahtarların kişiye özel olması ve unutulması durumunda sistemlere erişimin mümkün olmaması durumudur. Merkezi veri yapılarında şifrenin unutulması durumunda yeni şifre alınması adımları mevcuttur. Günümüzde kurulan hibrit sistemler hariç tüm genel ve özel blokzincir sistemlerinde kullanılan private key sağlamış olduğu güvenliğin yanı sıra kaybedilmesi durumunda saklanan kıymetli varlığın tümüyle kaybına sebebiyet verebilir.

Yukarıda da bahsettiğimiz %51 saldırısı teoride bir risk teşkil etmektedir. Günümüze kadar başarılı olmuş bir %51 saldırısı görülmemiştir. Ancak kuantum bilgisayarları marifetiyle yapılacak bir saldırının başarılı olma ihtimali yok sayılamaz. Bu sebeple %51 saldırısının bir dezavantaj olduğunu belirtmekte fayda vardır. İlerleyen süreçte kuantum hesaplama yöntemleriyle oluşturulan kriptoloji uygulamalarının hayata geçirilmesiyle %51 saldırıları bir risk olmaktan çıkacaktır.

Son olarak blokzinciri mimarisinin sağlamış olduğu kati şeffaflık, yanında mahremiyet sorununu birlikte getirmektedir (Tanrıverdi ve ark., 2019). Kriptoloji marifetiyle gizlenen kimlik bilgileri, açık olan işlem kayıtları takip edildiğinde tespit edilebilmektedir. Bu sebeple mahremiyet sorununun çözülmesi için hibrit çözümler üzerinde çalışılabilir.

3. Blokzinciri Teknolojisinin Türkiye'de Uygulanabileceği Alanlar

Blokzinciri teknolojisi; bankacılık uygulamaları, internet güvenliği, tedarik zinciri, nesnelerin interneti, sigortacılık, kişisel ve toplu ulaşım, online veri saklama, vakıf ve bağış işlemleri, oy verme süreçleri, kamu uygulamaları, sağlık uygulamaları, enerji yönetimi, fikri mülkiyet ve telif hakkı uygulamaları, emlak ve tapu uygulamaları, dijital kimlik, akıllı şehirler, akıllı sözleşmeler ve hukuki uygunluklarının incelenmesi, eğitim alanında uygulamaları gibi konularda uygulamaları mümkündür (Nguyen ve Dang, 2018). Ülkemizde de hemen hemen her alanda uyarlamalar yapılabilir ve blokzinciri hali hazırdaki sistemlere entegre edilebilir durumdadır. Çünkü Türkiye'nin gelişmekte olan bir ülke olması sebebiyle, ülkeye yatırım yapan firmalar marifetiyle bankacılıktan tedarik zincirlerine varıncaya kadar birçok alanda teknolojik yenilikler takip edilmiş, gerekli yatırımlar yapılmış ve yapılmaya devam etmektedir.

3.1. Bankacılık Uygulamaları

Blokzincirinin bankacılık alanında uygulamaları Bitcoin kripto parasının ortaya çıkması ve ilgi görmesinden sonra hız kazanmış bir çalışma alanıdır. Öncelikle kripto para alım satımlarının gerçekleştirilebilmesi üzerine çalışmalar yapılmıştır. Ayrıca günümüzde kripto paraların Forex sistemlerinde kaldıraçlı bir şekilde kullanımı mevcuttur. Ancak bu kullanımlar hali hazırda üretilmiş olan kripto paraların nakite çevrilmesi yahut ödeme olarak resmi kurumlara iletilmesinin kolaylaştırılması amacıyla yapılan çalışmalardır. Ayrıca özellikle Bitcoin'in ortaya çıkma mantığına ters bir ilerleyiş söz konusudur. Nitekim önerilmesinin arkasında yatan asıl sebeplerden biri bankalar gibi finans kurumlarının güvensiz atfedilip alternatif bir sistem kullanımının sağlanmasıdır. Gelinen noktada Bitcoin bankalar vasıtasıyla nakite çevrilen bir finansal enstrüman halini almıştır. Tüm bu kavramsal tezatlıklara rağmen ortada kullanımına ihtiyaç duyulan bir teknoloji bulunmaktadır. Türkiye'de bu alanda gerekli adımları atmaktadır. 23 Temmuz 2019 tarihinde Resmi Gazete'de yayımlanan 11.Kalkınma Planında; Blokzincir tabanlı dijital Merkez Bankası parası çıkarılma kararı alındığı görülmektedir (Resmi Gazete, 2019). İlerleyen süreçte pilot bölgelerde çalışan maaşlarının yahut kamuda açılan proje bedellerinin milli kripto para vasıtasıyla tahsil edilmesini görmek gayet doğaldır. Çünkü 2018 yılı verilerine göre kripto para konularında dünya çapında 63 merkez bankası, pratik ve teorik çalışmalar başlatmış durumda olup, bunların yüzde 10'u da pilot uygulamalara start verilmiştir (Tokyay, 2019). Yeni Zelanda gibi ülkelerde çalışan maaşlarının kripto paralar ile ödenmesinin önünün açıldığı bilinmektedir (URL-1, 2019).

Blokzincirinin bankacılık sistemlerinde kullanılmasının bir diğer alanı da kredi ve havale işlemleridir (Li ve ark., 2018). Kripto paralar dışında finansal enstrümanların transferinde blokzincir teknolojisi kullanılabilir (Ekbote ve ark., 2017). Ayrıca bankaların hali hazırdaki veri merkezlerini blokzinciri temelli hibrit yapılara çekilebilmesi mümkündür. Bu süreçler zorlu bir entegrasyon aşamalarını gerektireceği için süratli bir değişimin gerçekleşmesini beklemek gerçekçi bir bakış açısı olmaz. Ancak ülkemizde bu konularda çalışmalar yürütebilecek birçok devlet ve özel bankalar bulunmaktadır. Özellikle Yapı Kredi (URL-7, 2019) ve Garanti Bankası (URL-8, 2019) gibi kurumların sahip oldukları yazılım geliştirme birimleri, bu alanlarda yapılacak uyarlamaların altından kalkabilecek kapasitededir. Ayrıca TÜBİTAK BİLGEM Blokzinciri Araştırma Laboratuvarı, sahip olduğu kalifiye araştırmacı kadrosuyla benzer çalışmaları yürütebilecek yahut destek verebilecek potansiyele sahiptir.

Blokzincirinin finans sektöründe uygulanması para aklama ve illegal süreçlerin finanse edilmesinde kolaylık sağlayacağı düşüncesiyle, özellikle terörizm ve uyuşturucu ile mücadele eden merkezi otoritelerce kaygıyla karşılanmıştır. Bitcoin kripto parasındaki voladitenin sebebi yüksek

miktarlarda yapılan para aklama işlemleri ya da terörizmin finanse edilmesi gibi sebepler olabilir. Teknik olarak blokzincir sistemi düğümlerinin işlem yapma niyetlerini yargılayıp bir onay verme arayışında değildir. Ancak gözden kaçırılmaması gereken nokta bankacılık sektöründe blokzincir teknolojisinin uyarlanması bir Bitcoin blokzincir sisteminde olduğu gibi olmayacağıdır. Sisteme erişim sağlayan kişilerin bilgileri belirli oranda blokzincir sistemine geçirilecektir. İlerleyen süreçte karşılaşacağımız bankacılık sistemleri hibrit mantıkla üretilmiş ve tüm paydaşların mutabık kalacakları bir blokzincir bankacılık sistemi olacaktır. Ülkemizde kripto paraların dönüşüm işlemlerinin yapıldığı aracı internet sitelerinin yerini devlet ve özel bankaların alması gerekmektedir. Çünkü siber saldırganların başarılı oldukları tüm hırsızlık örnekleri internet takas sitelerinde gerçekleşmiştir. Uzman kadrolarca hazırlanmış sistemler üzerinde yapılacak kripto para transfer ve dönüşümleri büyük önem taşımaktadır ve ülkemizde bankalar marifetiyle bu ihtiyacın giderilmesi gerekmektedir.

3.2. İnternet Güvenliği

Günümüzde teknolojiye ve internete olan yüksek bağımlılık, kuruluşlar için yeni iş modelleri ve sistemlerin geliştirilmesi ile sonuçlanmıştır, ancak bununla birlikte siber saldırganların yararlanabileceği yeni boşluklar ve fırsatlar ortaya çıkmaktadır (Deloitte, 2017). Karşılaşılan bu boşluklardan doğan riskler sistemlerde belirli önlemler alındığı zaman en aza indirilebilir (Takaoğlu ve Özer, 2019). Ancak kesin bir korumadan bahsetmek mümkün değildir. Özellikle büyük veri tabanları olan şirketler, siber saldırganlarının ana hedefidir. Facebook gibi geniş bir ekiple çalışan ve gelişmiş saldırı tespit sistemleri olan bir kurum dahi 2018 Ekim'inde yapılan saldırılarda yeterli korumayı sağlayamamış ve 30 milyon insanın kullanıcı bilgileri çalınmıştır. Ülkemizde de benzer saldırılar geçmişte yaşanmış ve elde edilen bilgilerin derin web denilen ortamlarda satıldığı görülmüştür. Bu noktada blokzincir teknolojisi çözüm olarak düşünülebilir. İnternet teknolojisinin blokzincirine çekilmesi fikri yeni bir konu değildir. Bu alanda yapılan çalışmalar devam etmektedir. Ancak internetin blokzincirine çekilmesi süratle gerçekleşecek bir durum değildir. Bu sebeple saldırı tespit sistemlerinin blokzinciri temelli geliştirilmesi üzerine çalışılabilir. Ülkemizde geliştirilmiş ve dünya çapında başarılı olmuş yerli bir güvenlik programımız maalesef bulunmamaktadır. Bu sebeple Türkiye'de bu alanda yapılacak çalışmalara ihtiyaç duyulmaktadır.

3.3. Tedarik Zinciri

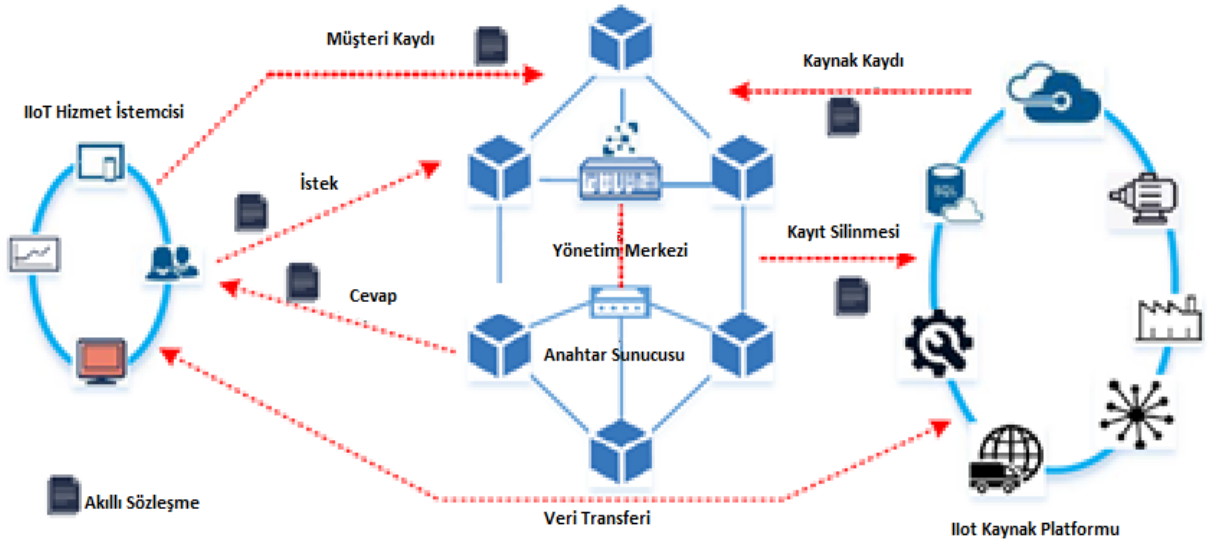
Lojistik, nakliye ve malzeme temini, blokzinciri teknolojisi için potansiyel uygulama alanları olarak sıklıkla adlandırılmıştır (Hinckeldeyn ve Kreutzfeldt, 2018). Blokzincirinin tedarik zincirinde kullanılması sayesinde tüm işlemler kayıt altına alınmış olup güvenli ve şeffaf bir şekilde takibi yapılabilmektedir. Toyota, AliBaba, Walmart, Provenance, JD.com gibi kurumlar blokzincir teknolojisini tedarik zincirinde başarıyla kullanmaya başlamışlardır (Kshetri ve Loukoianova, 2019). Örneğin blokzinciri tedarik zincirlerinde kullanılarak bir ürünün malzeme halinden bir ürüne dönüştürülmesi, ürünün satılmak amacıyla anlaşmalı firmalara iletilmesi, ürünün satıldıktan sonraki tüm garanti süresinin takibi ve yapılmışsa tamir işlemlerinin kaydı, ürünün el değiştirmesi durumunda yeni sahibinin sisteme girilmesi ve son olarak kullanılamaz hale gelip geri dönüşüme uğramasına varıncaya kadarki tüm adımlarının takibi yapılabilmektedir. Blokzinciri teknolojisi, güvenilir ve doğrulanmış bir lojistik sistemi ve tedarik zinciri bilgi alışverişi ağı sağlamaktadır (Dujak ve Sajter, 2019). Ülkemizde dağıtım ağı olan hemen hemen her sektörde kullanılabilir, olumlu geri dönüşler elde edilebilecek ve hızlıca kurulabilecek bir çalışma alanıdır.

3.4. Nesnelerin İnterneti

Kavramsal olarak açıklandığında, internete bağlanabilen tüm elektronik cihazların, bulut ağları aracılığıyla birbirleriyle bilgi paylaşımı yapması durumudur (Abbas ve Sung-Bong, 2019). Günümüzdeki mevcut nesnelerin interneti sistemler, çeşitli bulut teknolojisi ve cihazların değişen konfigürasyonları nedeniyle birlikte çalışabilirliği sınırlanan, güvene bağlı, merkezi bir bulut tabanlı modellerdir (Agrawal ve ark., 2018). 2020 yılında nesnelerin internetine bağlı cihazların sayısının 20 milyara ulaşacağı beklenmektedir (Özyılmaz ve Yurdakul, 2017). Başka bir değişle ilerleyen süreçte elektronik donanıma sahip tüm cihazların nesnelerin internetine bağlı bir hale geleceğinden bahsedilebilir. Nesnelerin interneti ağlarını güvenceye almak, dağıtılmış, heterojen ve kaynakların kısıtlı olması nedeniyle büyük bir zorluktur (Gupta ve ark., 2018). Bu sebeple güvenliğin sağlanmasında blokzincir sistemlerinin kullanılması üzerinde yapılan çalışmalar devam etmektedir. Blokzincir uyarlamaları yapılırken genellikle Ethereum temelli akıllı sözleşmelerden faydalanılmaktadır (Huh ve ark., 2017). Akıllı sözleşmeler özel bir durum için yazılan ve her seferinde aynı işlemi yaparak çalışan kodlardır. Dizayn edilirken çok dikkatli bir şekilde kodlanması gerekmektedir, çünkü bir akıllı sözleşme çalıştırıldığı anda yazılan kod kesinleşir ve değiştirilemez hale gelir (Papadodimas ve ark., 2018). Ethereum temelli bir akıllı sözleşme Solidity

programlama dilinde yazılır ve Ethereum Virtual Machine (EVM) kullanılarak derlenir (Fakhri ve Mutijarsa, 2018).

Nesnelerin birbiri ile gerçek zamanlı iletişim halinde olmasının sağlamakta olduğu faydalar sebebiyle birçok alanda kullanılmaya başlanmıştır. Özellikle sanayi uygulamalarında kullanılan nesnelerin internetinin güvenliğinin üst seviyeye çıkartılması için yapılan çalışmalar mevcuttur. Sanayide kullanımı için önerilmiş blokzincir entegreli nesnelerin interneti mimarisi Şekil 9'de paylaşılmıştır.



Şekil 9. Sanayide blokzincir tabanlı nesnelerin interneti mimarisi (Zhao ve ark., 2019)

Ülkemizde de nesnelerin interneti alanında yapılan birçok akademik çalışma bulunmaktadır. Akıllı evler, akıllı şehirler, akıllı sanayi gibi nesnelerin interneti sayesinde karşımıza çıkan tüm bu alanlarda Türkiye'de kaynakların daha verimli kullanılması, zamanın ve personelin doğru değerlendirilmesi açısından çalışmaların yapılmasına ihtiyaç duyulmaktadır. Yapılacak bu çalışmalarda blokzinciri entegreli sistemler geliştirilmesi ilerleyen süreçte karşılaşılabilecek güvenlik sorunlarının çözümü açısından büyük önem taşımaktadır.

3.5. Sigortacılık Uygulamaları

Türkiye'de ilk sigortacılık faaliyetleri 1872 yılında İngiliz sigorta şirketlerinin açtıkları temsilciliklerle başlamıştır (TSB, 2019). Günümüzde: Ferdi kaza sigortaları, hayat sigortaları, hırsızlık sigortası, kasko sigortası, mühendislik sigortaları, nakliyat sigortaları, sağlık sigortası, sorumluluk sigortaları, trafik sigortası, yangın sigortası, zorunlu deprem sigortası gibi birçok alanda sigortacılık hizmeti verilmektedir (TSB, 2019). Ayrıca ülkemizde Sigorta Bilgi ve Gözetim Merkezi

adı altında 5684 sayılı Sigortacılık Kanununun 31/B maddesinin birinci fıkrasına istinaden; sigortalılar ve sigorta sözleşmesinden dolaylı da olsa menfaat sağlayanlara ilişkin olarak, yanlış sigorta uygulamaları dâhil, risk değerlendirmesine esas bilgileri toplamak ve bu bilgilerin sigorta, reasürans ve sigortacılık faaliyetinde bulunan emeklilik şirketleri ile T.C. Hazine ve Maliye Bakanlığı'nca belirlenecek kişilerle paylaşılmasını sağlamak amacıyla kurulmuş, Bakanlık'ça belirlenen sigortalara ilişkin, poliçe, zeyil, hasar kayıtlarının sigorta şirketleri tarafından elektronik ortamdan transfer edilerek toplandığı bir bilgi merkezi bulunmaktadır (SBM, 2019). Anlaşılacağı üzere ülkemizdeki sigortacılık işlemlerinin bilgileri merkezi veri yapılarında saklanmaya devam etmektedir. Bu durum sigortacılık verilerini hedef haline getirmektedir. Blokzincir teknolojisi kullanarak hali hazırdaki veri yapılarının korunma altına alınması faydalı olacaktır. Ayrıca blokzinciri kullanılarak geliştirilmiş sigortacılık işlemlerinin veri güvenliği dışında sigorta firmalarına başka katkıları da bulunmaktadır. Sahte poliçelerle mücadele, fiyatlandırma doğruluğunun arttırılması, karlı müşteri hesaplarını tanımlamak, elde tutmak ve çekmek, dosya masraflarının azaltılması, müşterilere sadakat primlerini sağlama ve böylece daha fazlasını çekebilme (Kumar, Prasad ve Murthy, 2019), müşteri deneyiminin geliştirilmesi ve işletme maliyetlerinin azaltılması gibi katkılardır. Blokzinciri teknolojisini veri girişi ve kimlik doğrulama, prim hesaplama, risk değerlendirmesi, kullanım başına ödeme ve mikro sigorta gibi sigortacılık işlemlerine entegre etmek mümkündür (Gatteschi ve ark., 2018).

3.6. Kişisel ve Toplu Ulaşım

Günümüzde Uber uygulamasının elde ettiği başarı sonrası benzer birçok uygulama hayata geçirilmiştir. Ülkemizde de @taksi, Olev, BiTaksi, Scotty ve iTaksi gibi uygulamalar Uber benzeri yerli çözümler sunmaktadır. BlaBlaCar ve TAG (Tek Araba Gidelim) gibi araç sahipleriyle aynı yere gidecek kişilerle yol masraflarını paylaştığı uygulamalar da bulunmaktadır. Ayrıca yerli yabancı birçok araç kiralama firması da ülkemizde hizmet vermektedir. Toplu taşıma da dâhil olmak üzere belirtilen tüm alanlarda blokzincir uygulaması yapılabilmektedir. Blokzincirinin bir ürünü olan dijital cüzdanlar yardımıyla araç kiralama ücretleri, otobüs bilet ücretleri, tüm taksi uygulama ücretleri başta olmak üzere araçların akaryakıt, park ve geçiş ücretleri gibi tüm ödemeleri blokzincir dijital cüzdanları ile yapılabilmektedir. Blokzincirinin eşler arası iletişimi sağlayan yapısı sayesinde araç kiralama gibi işlemlerde aradan üçüncü bir şahsı çıkararak tüm ayrıntıların belirtildiği akıllı sözleşmeler oluşturulabilmektedir. Ülkemizde toplu taşımadan taksi uygulamalarına ve bireysel araç kiralamalara varıncaya kadar her alanda blokzinciri uygulama

çalışmalarına ihtiyaç bulunmaktadır. Dünyada UBS, ZF ve INNOGY gibi kuruluşlar bu alanda çalışmalar yürütmektedir (Nguyen ve Dang, 2018).

3.7. Online Veri Saklama

Online veri saklama işlemleri sağladığı avantajlar sebebiyle çoğunlukla bulut teknolojileri yardımıyla sürdürülmektedir. Büyük avantajlara rağmen bulut teknolojisinin güvenlik ve gizlilik endişeleri devam etmektedir (Jiang ve ark., 2019). Blokzincir teknolojisi, verileri ve diğer dijital ürünleri saklama ve paylaşma yöntemleriyle devrim yaratmaktadır (Uchibeke ve ark., 2018). Ayrıca literatürde yer almaya başlayan "Dağıtık İnternet" kavramı (Angeline ve ark., 2018) ile internetin blokzincirine çekilmesi çalışmaları yürütülmektedir. Bulut sistemlerinde karşılaşılan güvenlik ve gizlilik sorunlarına blokzinciri teknolojisi çözüm olabilecek yapıdadır. Bu alanda Storj, Siacoin, Filecoin, MaidSafe gibi blokzinciri kullanarak online veri saklama üzerine yürütülen projeler bulunmaktadır. Türkiye'de Vestel Cloud, Buluthan ve Cloudeos gibi yerli bulut teknolojisi hizmeti veren firmalar bulunmaktadır. Ancak bu uygulamalarda paylaşılmış bir blokzincir uyarlaması bilgisi bulunmamaktadır. Türkiye'de hali hazırda var olan yerli uygulamalar ve sıfırdan yapılacak blokzincir temelli, güvenli ve gizliliğin koruma altına alındığı veri saklama platformlarına ihtiyaç duyulmaktadır.

3.8. Vakıf ve Bağış İşlemleri

Her toplumda vakıf ve bağış kültürü bulunmaktadır. Küresel olarak düşünüldüğünde her yıl milyarlarca dolarlık bağışlar toplanmaktadır. Ülkemizde de vakfetme kültürü geçmişten gelen ve hukuksal zemini oturtulmuş bir gelenektir. Vakıf kuruluşlarının tüm işlemleri kanunlar çerçevesinde belirlenmiş olup sistematik bir şekilde takip edilmektedir. Ancak vakıflarda kamu vicdanına uygun olmayan durumlar yaşanabilmektedir. Özellikle toplanan bağışların harcanma yer ve şekilleri insanların akıllarında soru işaretleri bırakmaktadır. En küçük vakıftan dünya genelinde kabul görmüş yardım kuruluşlarına varıncaya kadar akla gelebilecek her kurumda gerek yüksek personel maaşları gerekse de fahiş fiyatlardan temin edilen gıda, ilaç, giyim gibi temel insani gereklerin alımında yapılan yolsuzluklar sebebiyle vakıf gelirleri israf edilmektedir. Bu sebeple vakıf işlemlerinin yüksek şeffaflık çerçevesinde yapılması gerekmektedir.

Üzerinde çalışmaya devam ettiğimiz Milli Bağış Zinciri Projesi gibi bir blokzincir sistemi ile Türkiye'de vakıfların başta yardım işlemleri olmak üzere üstlendikleri birçok görevin blokzincirine çekilmesi düşünülebilir. Örneğin yardıma ihtiyacı olan insanların bilgilerinin bulunduğu bir

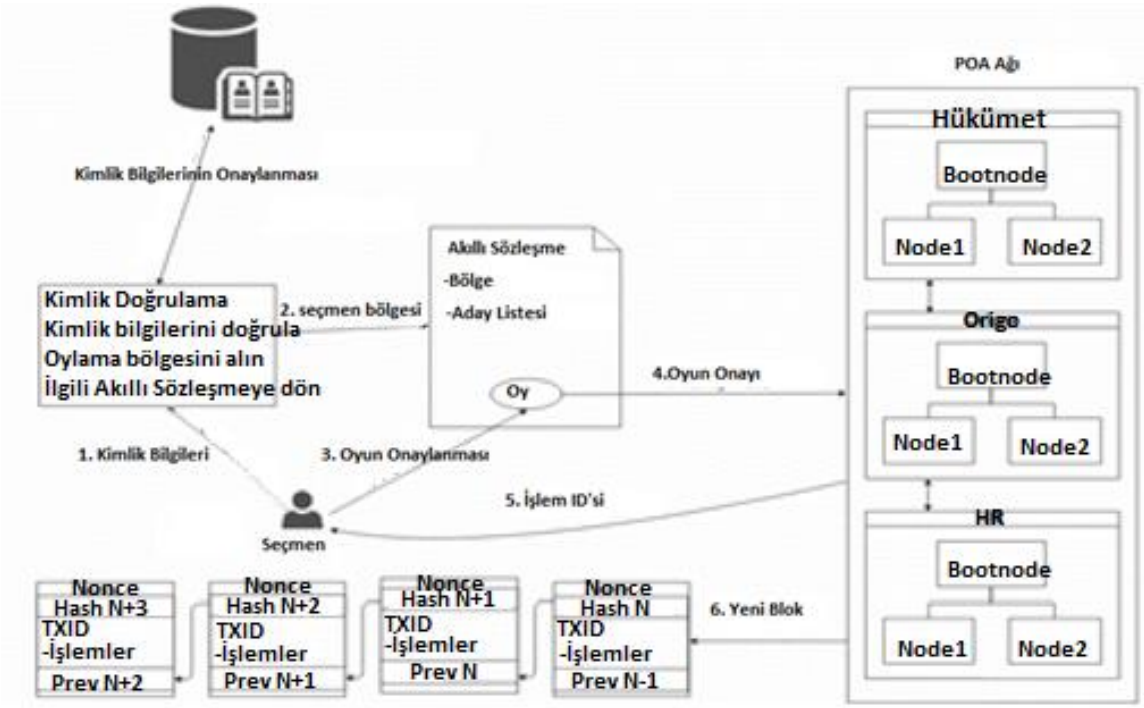
blokzinciri sayesinde bağışta bulunmak isteyen insanları arada hiçbir aracı bırakmadan direkt ihtiyaç sahipleriyle buluşturabilmek mümkündür. Blokzincir teknolojisi sayesinde kültürümüzde büyük önem atfedilen yapılan yardımın gizli tutulması geleneği sağlanırken, ihtiyaç sahibi insanların da muhtaçlık durumları gizlenmiş olur. Literatürde Türkiye'de bu alanda geliştirmekte olduğumuz çalışma dışında örnek bir proje bulunmamaktadır. Bu sebeple vakıf ve bağış işlemlerinin blokzinciri uyarlamaları dikkat çekilmesi gereken bir çalışma alanıdır.

3.9. Oy Verme Süreçleri

Seçim süreçleri dünyanın her yerinde ilgi çekici ve spekülasyonlara açık dönemlerdir. Seçim güvenliği, seçmen güvenliği, seçmenin seçime katılabilmesinin kolaylaştırılması (Wu ve Yang, 2018), hayatta olmayan ve seçime katılmayan seçmenler yerine oy kullanımı gibi problemler giderilmeye çalışılan sorunlardır. Bu tarz sorunların giderilmesi için ilk önerilen önerilerden biri elektronik seçim yapılmasıdır. Birçok ülkede seçimler bilgisayar vasıtasıyla seçim merkezlerinde yapılmaktadır. Ancak Amerika Birleşik Devletlerinde yaşanan son örnekte, yapılan seçimde siber saldırı sonucu başkanlığı onaylanan Donald Trump'ın kazandığı iddia edilmiştir. Bu iddia elektronik seçim sistemlerinin güvenilirliğinin sorgulanmasına sebebiyet vermiştir.

Blokzincir teknolojisi merkeziyetçi olmayan mimarisi sayesinde (Khoury ve ark., 2018) siber saldırıların etkinliğini yitirdiği, işlemlerin şeffaf bir şekilde tüm paydaşlarca görülebildiği için spekülasyondan uzak, oy kullanma hakkı olan kişiler tarafınca (Zhang ve ark., 2018) kullanılan oyun değiştirilme imkânı olmayacağı için tutarlı ve maksimum güvenilirliğin sağlandığı bir çözüm olarak karşımıza çıkmaktadır.

Teoride blokzincir tabanlı bir oylama sistemi kurmak çok basittir. Seçimin temel kurallarının belirlendiği Ethereum tabanlı bir akıllı sözleşme hazırlanır. Seçime giren adayların ve oy verebilme hakkına sahip vatandaşların belirlenmesi sonrasında adayların da dâhil oldukları, her seçmene bir dijital cüzdan oluşturulur. Bu cüzdanda tek bir coin bulunur ve seçmen istediği adaya cüzdanındaki coin transfer edilerek oy verme işlemini sonlandırır (Kshetri ve Voas, 2018). Şekil 10'da blokzincir temelli örnek bir oy verme işlemi paylaşılmıştır.



Şekil 10. Blokzincir altyapılı oy verme işlemi (Hjálmarsson ve ark., 2018)

Türkiye'de bilindiği üzere seçimler Yüksek Seçim Kurumu tarafından yapılmaktadır. Blokzinciri teknolojisi temelli milli bir seçim sistemi geliştirilmesi elbette kurumun yükünü hafifletecektir. Ayrıca oyların kati suretle güvenliği sağlanacağı için çokça karşılaşılan oy çalma iddiaları da son bulacaktır. Seçim sonuçlarından memnun olmayan her siyasi figürün suçu YSK ile ilişkilendirmesinin de önüne geçilecektir. Kısacası yapılan her seçimden sonra kamu gündemini meşgul eden tartışma konularının önüne geçilecektir.

Blokzincir temelli geliştirilen elektronik seçim sistemleri, dünyada çalışılan bir araştırma konusu olmakla birlikte ortaya örnekleri koyulmuş bir çalışma alanıdır. Geliştirilen sistemlerin gerçekleştirilen tüm seçimlerde kullanılabilir bir yapıya sahip olması sebebiyle çok geniş bir uygulama alanına sahiptir. Aşağıda Tablo 1'de literatürde karşılaşılan blokzincir tabanlı seçim uygulamalarının karşılaştırmalarına yer verilmiştir.

Tablo 1. Önerilmiş seçim mimarilerinin karşılaştırılması (Garg ve ark., 2019)

	Kimlik Doğrulama	Platform	Anonimlik	Seçmen Onayı	Dağıtık	Kullanılan Teknoloji
Biometric Aadhar Verification	Aadhar kart	Donanım	Evet	Evet	Kısmi Dağıtık	Biometric + Parmak izi okuyucusu
IOT Fingerprint	Parmak izi	Donanım	Evet	Evet	Kısmi Dağıtık	IOT + Parmak izi okuyucusu
Permissioned Blockchain	Evet	Yazılım	Evet	İzin	Dağıtık	Blokzincir
followmyvote	Yok	Web Tabanlı	Hayır	Hayır	Merkezi	Web Uygulaması
Estonian Voting System	Eid	Yazılım	Evet	Evet	Kısmi	-
DVBM	Posta	Web Tabanlı	Evet	Hayır	Kısmi	-
Norwegian I-voting system	MiniID	Yazılım	Evet	Evet	Kısmi	-
ivote	Posta	Web	Evet	Evet	Bilinmiyor	-
civitas	Posta	Yazılım	Evet	Evet	Evet	Java
Votebook (New York University)	Evet	Yazılım	Evet	-	Dağıtık	İzinli Blokzincir
Openvotebook Network (New York University)	Evet	Web Tabanlı	Evet	-	Dağıtık	Ethereum Blokzincir
The proposal of university of maryland	Evet	Donanım	Evet	-	Merkezi	ZKP ve Merkle Ağaçlı Ethereum Blokzincir
New South Wales iVote System	VoterID, PIN	Yazılım	Evet	Evet	-	-
Bronco Vote	Evet	Web Tabanlı	Evet	Evet	Evet	Ethereum Blokzincir
Plymouth Model	Evet	Yazılım	Evet	Evet	Evet	Blokzincir

3.10. Kamu Uygulamaları

Türkiye'de insanların kullanımına sunulan e-Devlet Kapısı uygulaması ile tüm kamu kurumlarıyla ilgili birçok işlem hızlı bir şekilde yapılmaktadır. Dünya'da emsal uygulamalar mevcuttur. Özellikle blokzincir temelli geliştirilen sistemler bu noktada ön plana çıkmaktadır. Birleşik Arap Emirlikleri 2020 yılında hükümet verilerinin blokzincir sistemine geçirileceğini duyurmuştur (Nguyen ve Dang, 2018). Ayrıca aktif olarak kullanılan en büyük blokzincir temelli kamu uygulaması Avrupa'da kullanılan TrustedChain'dir. Estonya ve Çin bazı kamu işlemlerinin blokzincir temelli sistemlerde yürütülmesine başlamıştır (Al-Megren ve diğerleri, 2018).

Blokzincir teknolojisinin para alışverişinin olduğu tüm devlet kurumlarında kullanılması durumunda şeffaflık ve hesap verebilirlik imkânı sağlanabileceği gibi kurumlarda karşılaşılan yozlaşma gibi sorunların önüne geçilebilmektedir (Mohite ve Acharya, 2018). Ülkemizde kullanılmakta olan E-Devlet Kapısı uygulamasının blokzincirine geçirilmesi üzerine çalışmalar yapılabilir.

3.11. Sağlık Uygulamaları

Blokzincir teknolojisinin kapasitesinin anlaşılması ve etki alanının gelişmesiyle teknolojinin uyarlanmaya çalışıldığı alanlardan biri de sağlık sektörü haline gelmiştir (Zheng ve ark., 2018). Hastanelerin iç mekanizmalarından doğan veri akışının güvence altına alınarak saklanması ve ilgili departmanlar arasında iletilmesi, hasta kayıtlarının saklanması ve ihtiyaç halinde diğer sağlık kurumlarınca erişilebilir olması (Sosu ve ark., 2019), ilaç takibinin yapılması ve ilaç sektöründe karşılaşılan sahtecilikle mücadele edilmesi, hastanın elektronik ekipmanlar vasıtasıyla gerçek zamanlı takibi (Attia ve ark., 2019), kan bankalarının bilgilerinin tüm paydaşlarla paylaşılması (Raju ve ark., 2017) gibi ihtiyaçlar bulunmaktadır. Bu sorunların çözümünde geleneksel veri saklama yöntemleri ve donanımlar kullanılarak ihtiyaçlar giderilmektedir.

Özellikle hastanelerde kullanılan veri merkezlerinin merkezi yapısı ve güvenlik protokollerinin yeteri kadar güçlü olmaması sebebiyle ciddi riskler ile karşılaşılmaktadır. Yürütmekte olduğumuz blokzincir temelli kalp pili verisi koruma projesi gibi çalışmaların ortaya çıkma sebebi, hali hazırda kullanılan veri merkezlerinin saldırıya açık yapıda olmalarıdır. Ayrıca bazı örneklerde hasta verilerinin hastane çalışanları tarafından sızdırıldığı görülmüştür. Bu sebeple hasta verilerinin saklanması ve acil tedavi gerektiren durumlar dışında hastanın izni olmadan kimse ile paylaşılmaması ve dışarıdan bir erişim ile verilerle oynanmaması (Ito ve ark., 2018) gerekmektedir. Şekil 11'de bu doğrultuda paylaşılmış örnek bir sağlıkta blokzincir uyarlaması paylaşılmıştır.

Şekil 11. Sağlıkta blokzincir uyarlaması (Wang ve ark., 2018)

Dünyada sağlık sistemlerinin blokzincirine çekilmesi konusunda çokça çalışmalar yürütülmektedir. Estonya teknolojik gelişmeleri yakından takip eden bir ülke olmakla birlikte sağlık alanında da blokzincir temelli X-Road (Martinson, 2019) sistemi yardımıyla hasta bilgilerini tutmaktadır. Hastalar sistemde kendi sağlık kayıtlarının mutlak sahibi olarak tanıtılmıştır. Hastanın izni olmadan verilerine üçüncü şahısların erişmesi cezai hükümlere bağlanmıştır (Ekin ve Ünay, 2018).

Massachusetts Institute of Technology Üniversitesinde başlatılan MedRec (Mertz, 2018) isimli çalışma ile Ethereum temelli akıllı sözleşmeler vasıtasıyla geliştirilmiş blokzincir sistemi ile hastaların EMR verilerinin hangi durum ve koşullarda, kimler tarafından erişilebileceğine dair izinlerin verilmesi üzerine çalışmalar yapılmaktadır. Ayrıca MediLedger, SimplyVitalHealth, Robomed Network, Healthureum, Gem, DokChain, MediBloc, BlockMedx, Patientory, MedicalChain gibi blokzincir temelli sağlık sistemleri kullanılmaktadır. Tablo 2'de yukarıda belirtilen sistemlerin detaylı bilgileri paylaşılmıştır.

Tablo 2. Blokzincir temelli sağlık bilgi sistemleri (Kombe ve ark., 2018).

Blokzincir Sistemi	**Blokzincir Tipi**	**Blokzincir Platformu**	**Akıllı Sözleşme Uygulaması**	**Token Kullanımı**	**Uygulama**
MedRec	Genel	Ethereum	Evet	Hayır	Sağlık verisi yönetimi
MediLedger	Konsorsiyum/Özel	Kısmi Ethereum	Evet	Hayır	Farmasötik Tedarik Zinciri
SimplyVital Health	Konsorsiyum	Health Nexus	Evet	Evet	Elektronik Sağlık Kayıtları
Robomed Network	Genel	Ethereum	Evet	Evet	Elektronik Sağlık Kayıtları
Healthureum	Genel	Ethereum	Evet	Evet	Sağlık Yönetimi
Gem	Hepsi	Hepsi	Hayır	Hayır	Hasta Verisi
DokChain	Konsorsiyum	Hyperledger Sawtooth	Evet	Evet	Finansal ve Hastane Verileri
MediBloc	Genel	QTum	Evet	Evet	Sağlık Veri Platformu
BlockMedx	Genel	Ethereum	Evet	Evet	Doktor Reçeteleri
Patientory	Genel	Ethereum	Evet	Evet	Elektronik Sağlık Verileri
MedicalChain	Konsorsiyum	Hyperledger Fabric, Ethereum (Token için)	Evet	Evet	Elektronik Sağlık Verileri

Türkiye'de ise e-Nabız sistemi ile kişisel sağlık bilgilerinin yönetilebileceği, güvenilir bir kişisel sağlık kaydı sistemi bulunmaktadır (TC Sağlık Bakanlığı, 2019). Ancak e-Devlet Kapısı uygulamasında olduğu gibi e-Nabız uygulaması da merkeziyetçi bir anlayışlar veriler saklanmaktadır. e-Nabız sisteminin blokzincirine çekilmesi üzerinde çalışılabilir. Ayrıca ülkemizde hatırı sayılır fazlalıkla özel hastaneler bulunmaktadır. Özel hastanelerin kendi sistemlerini blokzinciri temelli bir hale getirmeleri daha önce belirtilen sebeplerden ötürü büyük bir öneme sahiptir. Son olarak literatür incelendiğinde, Türkiye'de bu alanda akademik araştırmaların yapıldığı ve çalışmaların devam edildiği görülmektedir.

3.12. Enerji Yönetimi

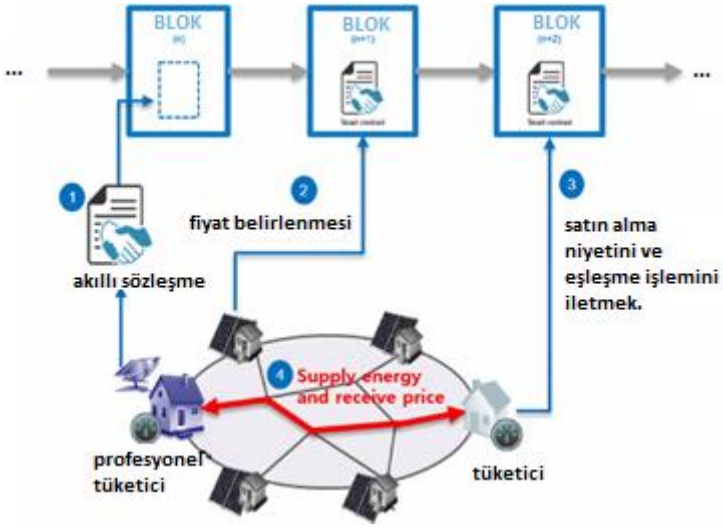
Blokzincir temelli akıllı kontratlar yardımıyla oluşturulan sistemler, enerjinin yönetimini çok daha şeffaf, verimli ve etkili bir şekilde sağlanabilmektedir (Chen ve ark., 2019). Konutların çatılarına kurulan güneş panellerinden üretilen elektrik enerjisinin kullanımından, rüzgâr panelleri,

jeneratörler ve çok daha büyük alanlarda enerji teminini sağlayan santrallere varıncaya kadar birçok alanda blokzincir sistemleri kullanılarak olumlu sonuçlar elde etmek mümkündür (Plaza ve ark., 2018). Hangi santralde ne kadar elektrik üretildiği, bunun ihtiyaç duyulan yerlere en hızlı ve verimli şekilde nasıl iletileceği de dâhil olmak üzere enerji dağıtımı sistematik bir şekilde izlenebilir ve dağıtım süreci kayıt altına alınabilir.

Elektrik enerjisi, üretildiği yerden uzak alanlara transfer edilmek istendiğinde kayıpların yaşandığı bir enerjidir. Bu sebeple İstanbul'da üretilen bir elektrik Ankara'ya gönderilmez. Üretilen enerjinin aynı bölgede kullanılmasının garanti altına alındığı durumlarda dahi enerji kayıplarıyla karşılaşılabilir. Bu sebeple bir bölgede, kayıp miktarı da eklenerek, kullanılması beklenen enerji miktarı hesaplanır ve fazlasının üretimine müsaade edilmez. Sistemler aşırı yüklenme durumunda kullanılamaz hale gelir ve kullanılmayan enerji de depolanamayacağı için üreticilerin sisteme göndermeleri gereken enerji miktarı çok önemlidir. Bu hesaplamaların ve takibin yapıldığı merkeziyetçi sistemler bulunmaktadır. Kullanılan sistemlerin merkeziyetçi bir yapıya sahip olunması sebebiyle sistemler saldırıların doğal bir hedefi haline gelmektedir.

Enerji santrallerine yapılan siber saldırılar yıkıcı sonuçlar doğurmaktadır. 2000 ve 2001 yıllarında California'da, 2015 yılında Ukrayna'da (Esfahani ve Mohammed, 2018) ve 2015 yılında ülkemizin de tecrübe ettiği bu tarz saldırılar hayatın akışını durdurmakta ve milyonlarca dolarlık zararlara neden olmaktadır. Bu sebeple elektrik dağıtım merkezlerinde siber güvenliğin yüksek olması gerekmektedir. Blokzincir teknolojisi sahip olduğu mimari sayesinde siber saldırı sorununa karşı doğal bir çözüm olarak karşımıza çıkmaktadır.

Literatür incelendiğinde yapılan birçok akademik çalışmanın yanı sıra Avustralya, Almanya ve Amerika Brooklyn'de enerji dağıtım işlemlerinin blokzincir temelli sistemlerce yapılması üzerine projelerle karşılaşılmıştır. Avustralya'da karşımıza çıkan PowerLedger projesi ile müşteriler istediği üreticiden elektrik temini yapmakta ve kullandıkları kadar enerji için bedel ödemektedirler. Brooklyn'de yapılan Brooklyn Microgrid adlı çalışma ile elektrik üretimi yapabilen komşular arasında herhangi bir elektrik üreticisi sözleşmeye dahil edilmeksizin enerji transferi yapılıp, akıllı sözleşmede belirlenen hükümler doğrultusunda ücretlendirme yapılmaktadır. Almanya'da ise RWE isimli enerji firması Slock.it isimli teknoloji firmasıyla birlikte geliştirdikleri BlockCharge isimli sistemle, batarya şarj işlemlerini takip eden ve kolayca ödeme işlemlerinin sağlayan bir projedir (Kim ve ark., 2018). Şekil 12'de blokzincir temelli örnek bir enerji dağıtım önerisi paylaşılmıştır.



Şekil 12. Enerji dağıtım süreci (Kang ve ark., 2018)

Türkiye'de blokzinciri sistemlerinden faydalanarak geliştirilmiş bir enerji yönetim sistemi bulunmamaktadır. Ayrıca ülkemizde EPDK, T.C. Enerji Piyasası Düzenleme Kurumu marifetiyle enerjinin yeterli, kaliteli, sürekli, ekonomik ve çevreyle uyumlu bir şekilde tüketiciye sunulması için düzenleme ve denetleme yapan bir kurum bulunmaktadır (EPDK, 2019). Literatürde EPDK'nın blokzincir temelli enerji yönetim sistemlerine geçeceğiyle ilgili bir bilgi ile karşılaşılmamıştır. Yenilenebilir enerji kaynaklarından elektrik üretiminin sağlandığı donanımların ekonomikleşmesi ve kırsalda kullanımının artması durumunda, blokzincir temelli sistemlerin kullanılmasının teşvik edilmesi faydalı olacaktır. Şahısların kendi marifetleriyle kurmuş oldukları yenilenebilir enerji üretim tesislerinde ürettikleri elektriği kendi ihtiyaçlarında kullanmaları ve fazla enerjilerini komşularına satma fikri çok cazip bir gelişmedir. Altyapı sağlanamayan yahut var olan eskimiş altyapıyı yenilemekte gecikmeler yaşanan bölgelerde Brooklyn'de yapılan örnekte olduğu gibi bir çalışma yapmak kısa sürede olumlu sonuçlar elde edilmesini sağlayabilir.

3.13. Fikri Mülkiyet ve Telif Hakkı Uygulamaları

Günümüzde karşılaşılan problemlerden birisi de fikri mülkiyet ve telif hakkı sorunlarıdır. Özellikle fotoğraf, müzik, film, video, edebi eserler, resim ve konusu bağımsız üzerinde çalışılan tüm projelerin fikri mülkiyet ve telif hakkı noktasında karşılaştıkları sorunlar bulunmaktadır. İnternet platformlarında çokça paylaşılan başkalarına ait dijital ürünlerin aidiyetleri ile ilgili karmaşıklıkların çözümünde günümüzde patent ve telif hakkı gibi sertifikasyonlar kullanılmaktadır. Ancak bu çözümler statik olup telif hakkı ödenmeden kullanılmış eserlerin ses getiren bir başarı elde etmesi durumunda tespiti yapılabilmekte ve yasal süreçler başlatılmaktadır.

Blokzincir teknolojisinin fikri mülkiyet ve telif haklarının korunması noktasında dağıtık ve değiştirilemez defter yapısı ve tüm katılımcıları tarafından şeffaf bir şekilde incelenebilmesi sayesinde kişilere ait olan tüm resim, müzik, edebi eserler, film ve senaryoları gibi telif hakkı kapsamına girebilecek her alanlarda çözüm sunmaktadır.

Resim ve fotoğraf gibi görsellerin haklarının korunması üzerine blokzincir temelli yapılan çalışmalar bulunmaktadır (Dong, 2018). Binded ve Vaultitute gibi çalışmalar blokzincir temelli çözümler sunmaktadır. Ancak bu sistemlerin sağlamış oldukları aidiyet bilgisinin merkezi otoritelerce kabul edilmesi gerekmektedir. Örneğin, çektiği fotoğrafları bu ve benzer uygulamalar kullanarak koruma altına aldığını düşünen bir fotoğrafçının hukuki bir aksilik olduğunda ispat olarak sunacağı bu kanıtın hukuken kabul edilmesi gerekmektedir.

Ülkemizde blokzincir teknolojisinden faydalanarak fikri mülkiyet ve telif hakkı korunması üzerine geliştirilmiş kamu ya da özel bir proje ile karşılaşılmamıştır. Bu alanda yerli çalışmalara ihtiyaç duyulmaktadır. Türk Patent Enstitüsü'nün vermekte olduğu patentlerin blokzincir sisteminde kaydederek paylaşılması üzerine bir çalışma faydalı olabilir.

3.14. Emlak ve Tapu Uygulamaları

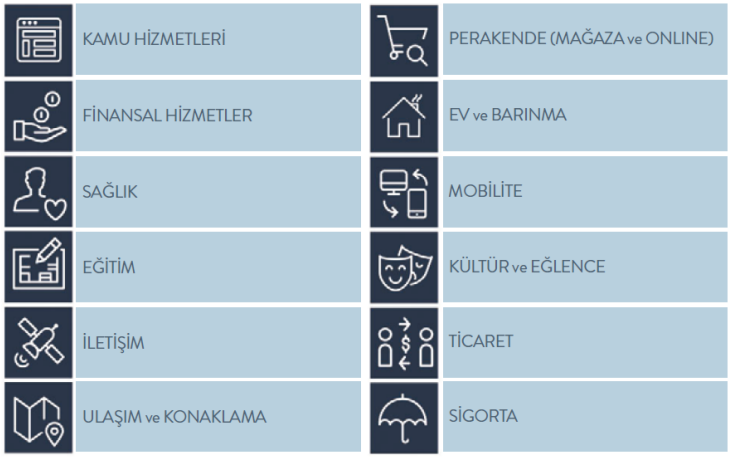
Türkiye'de emlak ve tapu uygulamaları Osmanlı'dan günümüze gelen süreçte düzgün işleyen alanlardan biridir. Yüzlerce yıl öncesinin tapusu arşivlerde kayıtlı bulunup aidiyeti bellidir. Günümüzde de gayrimenkul kayıt ve devir işlemleri Tapu ve Kadastro Genel Müdürlüğü'nce yapılmaktadır. Tapu ve Kadastro Müdürlüğünün sunmakta olduğu e-Randevu ve WebTapu gibi uygulamalarla işlemler sürdürülmektedir. Ayrıca emlak satışlarında yetkili tek kurum Tapu ve Kadastro Müdürlüğüdür, yani noter nezdinde yapılan anlaşmalar nihai değer taşımaz. Bu sebeple ülkemizde tapu işlemlerinin blokzinciri temelli bir sisteme geçirilmesi ancak Tapu ve Kadastro Müdürlüğünün gerekli görmesi durumunda yapılabilir. Ancak bu alanda yapılacak akademik çalışmalar, ilerleyen süreçte ihtiyaç duyulması durumunda yapılacak blokzinciri uyarlaması için kaynak olması sebebiyle önemlidir.

3.15. Dijital Kimlik

Türkiye'de dijital kimlik çalışmaları TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı tarafından yürütülmektedir. Dijital kimlik kavramı ile günümüzde kullanılan nüfus cüzdanları arasında teorik olarak hiçbir fark yoktur. Blokzincir temelli geliştirilen dijital kimlikler internete bağlı herhangi bir cihaz ile kullanılabilen kriptolojik ürünlerdir. Dünyada Amerika (URL-2, 2019),

Kanada (URL-3, 2019), Çin (URL-4,2019) ve Hindistan (URL-5, 2019)'da yapılmış çalışmalar bulunmaktadır. 2019 yılında gerçekleştirilen 2. Blokzincir Çalıştayında dijital kimlik çalışmalarının devam ettiği ve SSI Türkiye adı verilen dijital kimlik platformunun kurulacağının bilgisi paylaşılmıştır (URL-6, 2019).

Blokzincir temelli dijital kimlik cüzdanları sayesinde kimlik bilgilerinin gerektiği birçok alanda insanlar için kolaylıklar sağlanacaktır. Şekil 13'de dijital kimliklerin hangi ekosistemlerle etkileşim halinde olacağının bilgisi verilmiştir.



Şekil 13. Dijital kimlik kullanılabilecek ekosistemler (Blockchain Türkiye, 2019)

3.16. Akıllı Şehirler

Akıllı şehir kavramı, akıllı kamu hizmetleri, akıllı ulaşım, akıllı enerji, akıllı sağlık hizmetleri, akıllı tarım, akıllı eğitim kavramlarıyla direkt bağlantısı olan bir çalışma konusudur (Shuling, 2018). Nesnelerin interneti ve kablosuz sensor ağları konularının ilerlemesi sayesinde akıllı şehir fikri ortaya çıkmıştır (Kushch ve Prieto-Castrillo, 2019). Tüm ekosistemleriyle etkileşim halinde olan bir şehir fikri birçok sorunun çözümü olarak düşünülmektedir. Bulunduğumuz noktada ütopik gibi gözükse de ilerleyen süreçte akıllı şehir uygulamaları sayesinde trafik kazalarında, kalp krizi ve benzeri ani gelişen sağlık sorunları sebebiyle yaşanan ölüm olanlarında, öngörülemeyen gıda ve su ihtiyaçları sebebiyle karşılaşılan kıtlık, nüfus planlamasının doğru yapılamaması sebebiyle karşılaşılan eğitimde yetersiz altyapı ve istihdam oluşma gibi sorunlarda ciddi bir düşüş beklenmektedir. Şekil 14'te akıllı şehirlerin etkileşim halinde oldukları ekosistemler ile ilgili bir görsel paylaşılmıştır.

Şekil 14. Akıllı şehir bileşenleri. (Yetis ve Sahingoz, 2019)

Blokzincir teknolojisinin nesnelerin interneti konusunda kullanımının gerekliliği çalışmamızın 3.4. bölümünde paylaşılmıştır. Türkiye'de akıllı şehirler, kablosuz sensor ağları gibi konularda yapılan birçok akademik ve özel sektör çalışmaları bulunmaktadır. Ancak daha iyi bir şehir yönetimi ve planlamasının sağlanabilmesi için yükün ufak parçalara bölünüp kolayca çözülebilmesini sağlamak amacıyla ülkemizdeki tüm belediyeler nezdinde blokzincir temelli akıllı şehir uygulamalarının çalışılması gerekmektedir.

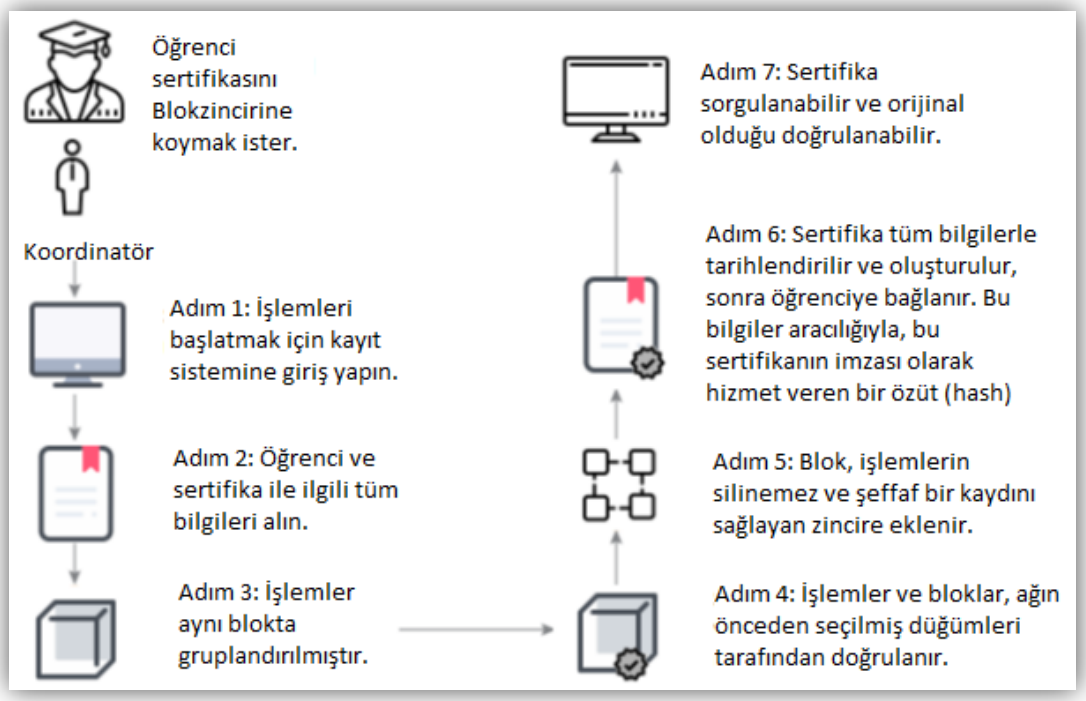
3.17. Akıllı Sözleşmeler ve Hukuki Uygunlukları

Akıllı sözleşmeler günümüzde karşılaşılan birçok soruna çözüm olmuştur. Adından da anlaşılacağı üzere "sözleşme" olan bu uygulamaların hukuksal bir karşılığı vardır. Bu noktada teknik bazı hukuksal sorunların olduğu literatürde görülmüştür. Örneğin borçlar hukuku ile ilgili yapılan çalışmada, kişilerin karşılıklı ya da tek taraflı olarak bir borç altına girebilmelerinde en önemli unsurun kişi iradesi olduğu ancak blokzincir temelli akıllı sözleşmelerde bu iradenin arka plana itildiği belirtilmiştir (Çekin, 2019). Bu ve benzer hukuki birçok uyumsuzluk, akıllı sözleşme uygulamalarının yaygınlaşmasıyla fark edilecek ve giderilmesi yönünde çalışmalar yapılacaktır. Türkiye'de bu alanda çalışan akademisyenler ve hukuk büroları bulunmaktadır. Ancak çalışmaların daha sistematik bir şekilde yapılabilmesi için çalışma konusu blokzincir teknolojisi ve hukuksal uygunlukları üzerine olan bir kurum kurulması faydalı olabilir.

3.18. Eğitim Alanında Uygulamaları

Günümüzde yüz yüze eğitim ve uzaktan eğitim adı altında birçok eğitim veren kurum bulunmaktadır. Verilen sertifikaların akrediteleri değişmekle birlikte edinilen belgeler katılımcılar için önem arz etmektedir. Ayrıca dünyada göç gibi bir gerçek bulunmaktadır. İnsanlar çeşitli sebeplerle yaşadıkları topraklardan ayrılmak durumunda kalmaktadırlar. Çoğu örnekte olduğu gibi göçmen statüsüne geçen insanların yerleştikleri ülkelerde aldıkları eğitimi ispat etmeleri gerekmektedir. Daha da önemlisi, kurumlara sunulan sertifika ya da diplomaların işverenler tarafından da doğrulanabilir olması gerekmektedir. Tüm bu sebeplerden ötürü blokzincir teknolojisi sayesinde sürdürülebilir bir çözüm getirilebilmektedir. Dünyanın neresinde olunursa olunsun kişilerin diploma, transkript ve sertifikalarının saklanacağı blokzincir temelli sistemler sayesinde erişim ve doğrulama işlemleri yapılabilmektedir. Dünyada blokzinciri eğitimi vermek ve farklı alanlarda uygulamalarını hayata geçirmek amacıyla birçok üniversite ve özel sektör kurumu çalışmalarını sürdürmektedir. Eğitim ile ilgili konularda geliştirilen; EduCTX, ODEM, Blockcerts, BitDegree, Disciplina, EdChain, NTOK, Academy, EduCoin, LiveEdu, Experty, EdgeCoin ve KryptEd gibi projeler bulunmaktadır (Yıldırım, 2018).

Ülkemizde de blokzincir konusunun önemi üniversitelerce fark edilmiş ve bu alanda Gebze Teknik Üniversitesi, Kadir Has Üniversitesi, İstanbul Ticaret Üniversitesi, Antalya Bilim Üniversitesi, İstanbul Gedik Üniversitesi, Ankara Yıldırım Beyazıt Üniversitesi, Konya Necmettin Erbakan Üniversitesi, Bahçeşehir Üniversitesi, Marmara Üniversitesi ve İstanbul Aydın Üniversitesinde blokzincir teknolojisi üzerine çalışmalar yapılmaktadır. Şekil 15'de eğitimde kullanılması için önerilmiş bir blokzincir uygulaması paylaşılmıştır.



Şekil 15. Eğitimde blokzincir uygulaması (Bessa ve Martins, 2019)

4. Sonuç

Çalışmamızda blokzincir teknolojisi, kapsamlı bir literatür taramasıyla araştırılmıştır. Blokzincir teknolojisinin tarihi gelişimi, teknik anlatımı, günümüzde teknolojinin sağladığı avantaj ve dezavantajlar açıklanmıştır. Blokzincir teknolojisinin literatürde karşılaşılan uygulama alanları tespit edilmiştir. Ülkemizde uygulanabilecek blokzincir çalışma alanları belirlenmiştir. Belirlenen çalışma konularında Türkiye'de hali hazırda yürütülmekte olan projeler paylaşılmıştır. Literatür taramasında çalışıldığı görülmemiş konuların Türkiye'de hangi alanlarda uygulanabileceği ile ilgili görüşlere yer verilmiştir.

Blokzincir teknolojisi Türkiye'de başında yakalanmış bir çalışma konusudur. Yapılan teorik çalışmalar incelendiğinde, dünyadaki emsalleriyle paralel yürütülen, arada çok büyük farkların olmadığı sonuçlarla karşılaşılmaktadır. Uygulama örneklerinde ise maalesef yavaş sonuçlar alındığı görülmektedir. Ayrıca çalışmamızda da belirttiğimiz üzere dijital kimlik, online veri saklama, kişisel ve toplu ulaşım ve finansal uygulamalar dışındaki alanlarda üretilmiş yerli ürünlerin çok az olduğu ve doğal olarak bu alanlarda teorik çalışmalar dışında projelendirilmiş yazılım uygulamalarının olmadığı görülmektedir.

Çalışmamızda yapılan araştırmalar sonucunda, blokzincir teknolojisinin ilerleyen süreçte Türkiye'de çokça kullanılan ve yeni uygulama alanlarının tespit edileceği bir çalışma konusu olacağını düşünmekteyiz. Blokzincir araştırma merkezlerinin sayısının arttırılması, kalifiye yazılımcıların istihdam edilmesi, üniversitelerde blokzincir üzerine verilen derslerin yaygınlaşması ve bu alanda çalışan merkezlerin finanse edilmesi durumunda daha hızlı sonuçlar alınacağını düşünmekteyiz.

Kaynaklar

Abbas, Q. E. ve Sung-Bong, J. (2019). A Survey of Blockchain and Its Applications. *International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Okinawa, Japan, (pp. 001-003). doi: 10.1109/ICAIIC.2019.8669067.

Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A. ve Shekhar, S. (2018). Continuous Security in IoT Using Blockchain. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, (pp. 6423-6427). doi: 10.1109/ICASSP.2018.8462513.

Al-Megren, S., Alsalamah, S., Altoaimy, L., Alsalamah, H., Soltanisehat, L., Almutairi, E. ve Pentland, A. S. (2018). Blockchain Use Cases in Digital Sectors: A Review of the Literature. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, (pp. 1417-1424). doi: 10.1109/Cybermatics_2018.2018.00242.

Angeline, R., Nathan, P. ve Karan, G. (2018). An immortal database system for the decentralized internet. *3rd International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, (pp. 994-998). doi: 10.1109/CESYS.2018.8723990.

Aste, T., Tasca, P. ve Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer*, 50(9), 18-28. doi: 10.1109/MC.2017.3571064.

Attia, O., Khoufi, I., Laouiti, A. ve Adjih, C. (2019). An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application. *10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Canary Islands, Spain, (pp. 1-5). doi: 10.1109/NTMS.2019.8763849.

Balaskas, A. ve Franqueira, V. N. L. (2018). Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow, (pp. 1-8). doi: 10.1109/CyberSecPODS.2018.8560672.

Belotti, M., Božić, N., Pujolle G. ve Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which and How. *in IEEE Communications Surveys & Tutorials.* doi: 10.1109/COMST.2019.2928178.

Bessa, E. E. ve Martins, J. S. B. (2019). A Blockchain-based Educational Record Repository. *7th International Workshop on Advances in ICT*. DOI: 10.5281/zenodo.2567524. Web Site: https://hal.archives-ouvertes.fr/hal-02085749/document.

Bhat, M. ve Vijayal, S. (2017). A Probabilistic Analysis on Crypto-Currencies Based on Blockchain. *International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, Jammu, (pp. 69-74). doi: 10.1109/ICNGCIS.2017.37.

Blockchain Türkiye (2019). Dijital Kimlik, Blockchain Türkiye Platformu Finans, Bankacılık ve Sigortacılık Çalışma Grubu Raporu. Web site: https://bctr.org/rapor-blockchain-ve-dijital-kimlik-8885/.

Chen, S., Guo, B., Yan, H., Qin, Q., Li, B. ve Qi, B. (2019). Application and Prospect of Integrated Energy Interoperability Management System Based on Blockchain. *IEEE International Conference on Energy Internet (ICEI)*, Nanjing, China, (pp. 421-425). doi: 10.1109/ICEI.2019.00080.

Çekin, M. S. (2019). Borçlar Hukuku ile Veri Koruma Açısından Blokchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı? *İstanbul Hukuk Mecmuası*, 77(1), 315-341.

Deloitte (2017). Blockchain and Cybersecurity. An assessment of the security of blockchain Technology. Web site: https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html.

Dinh, T., T., A., Liu, R., Zhang, M., Chen, G., Ooi, B. C. ve Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *in IEEE Transactions on Knowledge and Data Engineering*, 30(7), (pp. 1366-1385), doi: 10.1109/TKDE.2017.2781227.

Dong, X. (2018). A method of image privacy protection based on blockchain technology. *International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, Fuzhou, China, (pp. 1-4). doi: 10.1109/ICCBB.2018.8756447.

Duan, H., Zheng, Y., Du, Y., Zhou, A., Wang, C. ve Au, M. H. (2019). Aggregating Crowd Wisdom via Blockchain: A Private, Correct, and Robust Realization. *IEEE International Conference on Pervasive Computing and Communications PerCom*, Kyoto, Japan, (pp. 1-10). doi: 10.1109/PERCOM.2019.8767412.

Dujak, D. ve Sajter, D. (2019). Blockchain Applications in Supply Chain. *In: Kawa A., Maryniak A. (eds) SMART Supply Network. EcoProduction (Environmental Issues in Logistics and Manufacturing)*. Springer, Cham, (pp. 21-46). doi: 10.1007/978-3-319-91668-2_2.

Ekbote, B., Hire, V.D., Mahajan, P.G. ve Sisodia, J. (2017). Blockchain based remittances and mining using CUDA. *International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, (pp. 908-911). doi:10.1109/smarttechcon.2017.8358503.

Ekin, A. ve Ünay, D. (2018). Blockchain applications in healthcare. *26th Signal Processing and Communications Applications Conference (SIU)*, İzmir, (pp. 1-4). doi: 10.1109/SIU.2018.8404275.

EPDK (2019). T.C. Enerji Piyasası Düzenleme Kurumu. Web site: https://www.epdk.org.tr/.

Esfahani, M. M. ve Mohammed, O. A. (2018). Secure Blockchain-Based Energy Transaction Framework in Smart Power Systems. *IECON - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, (pp. 260-264). doi: 10.1109/IECON.2018.8591779.

Fakhri, D. ve Mutijarsa, K. (2018). Secure IoT Communication using Blockchain Technology, *International Symposium on Electronics and Smart Devices (ISESD)*, Bandung, (pp. 1-6). doi: 10.1109/ISESD.2018.8605485.

Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K. ve Gupta, S. (2019). A Comparitive Analysis on E-Voting System Using Blockchain. *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, (pp. 1-4). doi: 10.1109/IoT-SIU.2019.8777471.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. ve Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?. *Future Internet.* 10(2), 20. doi:10.3390/fi10020020.

Golosova, J. ve Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. *IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius, (pp. 1-6). doi: 10.1109/AIEEE.2018.8592253.

Gupta, Y., Shorey, R., Kulkarni, D. ve Tew, J. (2018). The applicability of blockchain in the Internet of Things. *10th International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, (pp. 561-564). doi: 10.1109/COMSNETS.2018.8328273.

Hinckeldeyn, J. ve Jochen, K. (2018). (Short Paper) Developing a Smart Storage Container for a Blockchain-Based Supply Chain Application. *Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, (pp. 97-100). doi: 10.1109/CVCBT.2018.00017.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M. ve Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, (pp. 983-986). doi: 10.1109/CLOUD.2018.00151.

Huh, S., Cho, S. Ve Kim, S. (2017). Managing IoT devices using blockchain platform. *19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, (pp. 464-467). doi: 10.23919/ICACT.2017.7890132.

Ito, K., Tago, K. ve Jin, Q. (2018). i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data. *9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, (pp. 829-833). doi: 10.1109/ITME.2018.00186.

Jiang, S., Liu, J., Wang, L. ve Yoo, S. (2019). Verifiable Search Meets Blockchain: A Privacy-Preserving Framework for Outsourced Encrypted Data. *IEEE International Conference on Communications (ICC)*, Shanghai, China, (pp. 1-6). doi: 10.1109/ICC.2019.8761146.

Kang, E. S., Pee, S. J., Song, J. G. ve Jang, J. W. (2018). A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid. *3rd International Conference on Computer and Communication Systems. (ICCCS)*, Nagoya, Japan, (pp. 472-476). doi: 10.1109/CCOMS.2018.8463317.

Khoury, D., Kfoury, E. F., Kassem, A. ve Harb, H. (2018). Decentralized Voting Platform Based on Ethereum Blockchain. *IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, Beirut, (pp. 1-6). doi: 10.1109/IMCET.2018.8603050.

Kim, G., Park, J. ve Ryou, J. (2018). A Study on Utilization of Blockchain for Electricity Trading in Microgrid. *IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai, (pp. 743-746). doi: 10.1109/BigComp.2018.00141.

Kolekar, S. M., More, R. P., Bachal, S. S. ve Yenkikar, A. V. (2018). Review Paper on Untwist Blockchain: A Data Handling Process of Blockchain Systems. *International Conference on Information, Communication, Engineering and Technology (ICICET)*, Pune, India, (pp.1-4). doi: 10.1109/ICICET.2018.8533868.

Kombe, C., Dida, M. ve Sam, A. (2018). A review on healthcare information systems and consensus protocols in blockchain technology. *International Journal of Advanced Technology and Engineering Exploration.* 5(49), 473-483. doi:10.19101/IJATEE.2018.547023.

Kshetri, N. ve Loukoianova, E. (2019). Blockchain Adoption in Supply Chain Networks in Asia. *in IT Professional*, 21(1), 11-15. doi: 10.1109/MITP.2018.2881307.

Kshetri, N. ve Voas, J. (2018). Blockchain-Enabled E-Voting. *in IEEE Software*, 35(4), 95-99. doi: 10.1109/MS.2018.2801546.

Kushch, S. ve Prieto-Castrillo, F. (2019). Blockchain for Dynamic Nodes in a Smart City. *IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, (pp. 29-34). doi: 10.1109/WF-IoT.2019.8767336.

Kumar, A., Prasad, A. ve Murthy, R. (2019). Application of Blockchain in Usage Based Insurance. *International Journal of Advance Research, Ideas and Innovations in Technology, IJARIIT*. 5(2), 1574-1577.

Lee, J. H. (2018). Blockchain Technologies: Blockchain Use Cases for Consumer Electronics. *in IEEE Consumer Electronics Magazine*, 7(4), 53-54. doi: 10.1109/MCE.2018.2816278.

Liu, Q. ve Li, K. (2018). Decentration Transaction Method Based on Blockchain Technology, *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, Xiamen, (pp. 416-419). doi: 10.1109/ICITBS.2018.00111.

Li, Y., Liang, X., Zhu, X. ve Wu, B. (2018). A Blockchain-Based Autonomous Credit System. *IEEE 15th International Conference on e-Business Engineering (ICEBE)*, Xi'an, (pp. 178-186). doi: 10.1109/ICEBE.2018.00036.

Lou, J., Zhang, Q., Qi, Z. ve Lei, K. (2018). A Blockchain-based key Management Scheme for Named Data Networking. *1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, Shenzhen, (pp. 141-146). doi: 10.1109/HOTICN.2018.8605993.

Ma, Z., Huang, W., Bi, W., Gao, H. ve Wang, Z. (2018). A master-slave blockchain paradigm and application in digital rights management. *in China Communications*, 15(8),174-188. doi: 10.1109/CC.2018.8438282.

Martinson, P. (2019). Estonia – the Digital Republic Secured by Blockchain. *Aktsiaselts PricewaterhouseCoopers*, PwC. Web sitesi: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

Mertz, L. (2018). (Block) Chain Reaction. *IEEE Pulse. A Magazine of The IEEE Engineering in Medicine and Biology Society*. Web sitesi: https://pulse.embs.org/may-2018/blockchain-reaction-healthcare/.

Miraz, M. H. ve Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. *Annals of Emerging Technologies in Computing (AETiC)*, 2(1), 1-6.

Mitra, R. (2019). Complete Guide to Big Data and Blockchain. Web site: https://blockgeeks.com/guides/big-data-and-blockchain/.

Mohite, A. ve Acharya, A. (2018). Blockchain for government fund tracking using Hyperledger. *International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, Belgaum, India, (pp. 231-234). doi: 10.1109/CTEMS.2018.8769200.

Nadiya, U., Mutijarsa, K. ve Rizqi, C. Y. (2018). Block Summarization and Compression in Bitcoin Blockchain. *International Symposium on Electronics and Smart Devices (ISESD)*, Bandung, (pp. 1-4). doi: 10.1109/ISESD.2018.8605487.

Nakamoto, S. (2008). Bitcoin: A Peer to Peer Electronic Cash System. Web sitesi: https://bitcoin.org/bitcoin.pdf.

Nguyen, Q. K. ve Dang, Q. V. (2018). Blockchain Technology for the Advancement of the Future. *4th International Conference on Green Technology and Sustainable Development*. (pp. 483-486). doi: 10.1109/GTSD.2018.8595577.

Nishith Desai Associates (2016). Beyond Bitcoin: Exploring the Blockchain | Industry Applications and Legal Perspectives. Nishith Desai Associates. Web sitesi: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Bitcoins.pdf.

Özyılmaz, K. R. ve Yurdakul, A. (2017). Work-in-progress: integrating low-power IoT devices to a blockchain-based infrastructure. *International Conference on Embedded Software (EMSOFT)*, Seoul, (pp. 1-2). doi: 10.1145/3125503.3125628.

Papadodimas, G., Palaiokrasas, G., Litke, A. ve Varvarigou, T. (2018). Implementation of smart contracts for blockchain based IoT applications. *9th International Conference on the Network of the Future (NOF)*, Poznan, (pp. 60-67). doi: 10.1109/NOF.2018.8597718.

Ra, G. ve Lee, I. (2019). A Study on Hybrid Blockchain-based XGS (XOR Global State) Injection Technology for Efficient Contents Modification and Deletion. *Sixth International Conference on Software Defined Systems (SDS)*, Rome, Italy, (pp. 300-305). doi: 10.1109/SDS.2019.8768696.

Plaza, C., Gil, J., Chezelles, F. ve Strang, K. A. (2018). Distributed Solar Self-Consumption and Blockchain Solar Energy Exchanges on the Public Grid Within an Energy Community. *IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Palermo, (pp. 1-4). doi: 10.1109/EEEIC.2018.8494534.

Raju, S., Rajesh, V. ve Deogun, J. S. (2017). The Case for a Data Bank: an Institution to Govern Healthcare and Education. *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance*, New Delhi AA, India, (pp. 538-539). doi: 10.1145/3047273.3047275.

Resmi Gazete (2019). 23 Temmuz 2019 tarihli 11. Kalkınma Planı. Web sitesi: https://www.resmigazete.gov.tr/eskiler/2019/07/20190723M1-1.htm.

Salah, K., Rehman, M. H. U., Nizamuddin, N. ve Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. *in IEEE Access*, 7, 10127-10149. doi: 10.1109/ACCESS.2018.2890507.

Saltykov, S. A. ve Rusyaeva, E. Yu. (2018). Theory Game as Priority Area of Researches for Development of Blockchain Technology. *Eleventh International Conference Management of large-scale system development MLSD*, Moscow, (pp. 1-4). doi: 10.1109/MLSD.2018.8551854.

SBM, (2019). Sigorta Bilgi ve Gözetim Merkezi. Web sitesi: https://www.sbm.org.tr/tr/sayfa/sbm-hakkinda-63.

Shuling, L. (2018). Application of Blockchain Technology in Smart City Infrastructure. *IEEE International Conference on Smart Internet of Things (SmartIoT)*, Xi'an, (pp. 266-276). doi: 10.1109/SmartIoT.2018.00056.

Singh, M., Singh, A. ve Kim, S. (2018). Blockchain: A game changer for securing IoT data. *IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, (pp. 51-55). doi: 10.1109/WF-IoT.2018.8355182.

Sosu, R. N. A., Quist-Aphetsi, K. ve Nana, L. (2019). A Decentralized Cryptographic Blockchain Approach for Health Information System. *International Conference on Computing, Computational Modelling and Applications (ICCMA)*, Cape Coast, Ghana, (pp. 120-1204). doi: 10.1109/ICCMA.2019.00027.

Szabo, N. (1994). Smart contracts. Web sitesi: http:/szabo.best.vwh.net.

Takaoğlu, M. ve Özer, Ç. (2019). Saldırı Tespit Sistemlerine Makine Öğrenme Etkisi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 3(1), 11-22. doi: 10.33461/uybisbbd.558192.

Takaoğlu, M., İşler, B. ve Küçükali, U. F. (2019). Blokzinciri ve Kripto Paraların İnsanlığa Etkileri. *e-Yeni Medya Dergisi / Yeni Medya Elektronik Dergi – eJNM*, 3(2), 71-83.

Tanrıverdi, M., Uysal, M. ve Üstündağ, M. T. (2019). Blokzincir Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217.

TC Sağlık Bakanlığı (2019). e-Nabız Kişisel Sağlık Sistemi. Web sitesi: https://enabiz.gov.tr/Yardim/Index.

Tokyay, M. (2019). Merkez Bankası yerli dijital para hazırlığında: Türk kripto parası başarılı olur mu? Web sitesi: https://tr.euronews.com/2019/07/13/merkez-bankasi-yerli-dijital-para-hazirliginda-kripto-para-enflasyon-guven-ekonomik-kriz.

TSB, (2019). Türkiye Sigorta Birliği. Web sitesi: https://www.tsb.org.tr/turkiyede-sigortacilik.aspx?pageID=439.

Uchibeke, U. U., Schneider, K. A., Kassani S. H. ve Deters, R. (2018). Blockchain Access Control Ecosystem for Big Data Security. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, (pp. 1373-1378). doi: 10.1109/Cybermatics_2018.2018.00236.

URL-1:https://qz.com/1687151/new-zealands-tax-authority-approves-crypto-wages-and-salaries/ (Erişim Tarihi: 30 Ekim 2019).

URL-2: https://verified.me/ (Erişim Tarihi: 1 Kasım 2019).

URL-3: https://www.uport.me/ (Erişim Tarihi: 1 Kasım 2019).

URL-4: http://www.idhub.network/en/(Erişim Tarihi: 1 Kasım 2019).

URL-5: https://uidai.gov.in/ (Erişim Tarihi: 1 Kasım 2019).

URL-6:https://uekae.bilgem.tubitak.gov.tr/tr/haber/2-ulusal-blokzincir-calistayi-bilgembw2019-gerceklestirildi) (Erişim Tarihi: 1 Kasım 2019).

URL-7: https://code.yapikredi.com.tr/anasayfa (Erişim Tarihi: 7 Aralık 2019).

URL-8: https://www.garantiteknoloji.com.tr/ (Erişim Tarihi: 7 Aralık 2019).

Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y.,Ouyang, L.,Guo, Y. ve Wang, F.Y. (2018). Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *in IEEE Transactions on Computational Social Systems*, 5(4), 942-950. doi: 10.1109/TCSS.2018.2865526.

Wu, H. ve Yang, C. (2018). A Blockchain-Based Network Security Mechanism for Voting Systems, *1st International Cognitive Cities Conference (IC3)*, Okinawa, (pp. 227-230). doi: 10.1109/IC3.2018.00-15.

Yetis R. ve Sahingoz, O. K. (2019). Blockchain Based Secure Communication for IoT Devices in Smart Cities. *7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, Istanbul, Turkey, (pp. 134-138). doi: 10.1109/SGCF.2019.8782285.

Yıldırım, H. (2018). Açık ve uzaktan öğrenmede blokzincir teknolojisi kullanımı. *Açık öğretim Uygulamaları ve Araştırma Dergisi*, *AUAd*, 4(3), 142-15.

Zhang, W., Huang, S., Yuan, Y., Hu, Y., Huang, S., Cao, S. ve Chopra, A. (2018). A Privacy-Preserving Voting Protocol on Blockchain. *in IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, (pp. 401-408). doi: 10.1109/CLOUD.2018.00057.

Zhao, S., Li, S. ve Yao, Y. (2019). Blockchain Enabled Industrial Internet of Things Technology. *in IEEE Transactions on Computational Social Systems*. (pp. 1-12). doi: 10.1109/TCSS.2019.2924054.

Zheng, K., Liu, Y., Dai, C., Duan, Y. ve Huang, X. (2018). Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network. *9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, (pp. 877-881). doi: 10.1109/ITME.2018.00196.