Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Blockchain Tabanlı Bir Veri Yönetim Modeli

Mohammed ALSADİ[a], Sevinç GÜLSEÇEN[b], Sinan KARA[c], Büşra ÖZDENİZCİ KÖSE[*,d], Vedat COŞKUN[e]

[a,*] *Enformatik Bölümü, İstanbul Üniversitesi, İSTANBUL, 34134, TÜRKİYE*
[b] *Enformatik Bölümü, İstanbul Üniversitesi, İSTANBUL, 34134, TÜRKİYE*
[c] *Turkcell Teknoloji Araştırma ve Geliştirme, İSTANBUL, 34854, TÜRKİYE*
[d] *İşletme Bölümü, Gebze Teknik Üniversitesi, KOCAELİ, 41400, TÜRKİYE*
[e] *Yazılım Mühendisliği, Beykent Üniversitesi, İSTANBUL, 34398, TÜRKİYE*

MAKALE BİLGİSİ

Alınma: 04.11.2019
Kabul: 23.12.2019

Anahtar Kelimeler:
Blockchain, IoT, Akıllı Ulaşım, Bağlantılı Araç

Sorumlu Yazar
e-posta:
busraozdenizci@gtu.edu.tr

ÖZET

Nesnelerin İnterneti (Internet of Things, IoT), fiziksel nesnelere birtakım algılama, görme, uyarma gibi yeteneklerin kazandırılması ve nesnelerin birbiri ile iletişim kurabilmesine olanak sağlamaktadır. Akıllı nesne kaynaklarının ve iletişim ağ yeteneklerinin gelişimiyle, çeşitli akıllı ortamlar –sağlık, şebeke, ev, fabrika, tarım, şehir, araçlar, ulaşım ve benzeri- hızla gelişmektedir. Bu kapsamda, IoT sistemlerinde işlenecek verilerin ve gerçekleştirilecek işlemlerin güvenliği ve gizliliği oldukça önemli bir konudur. Çalışmamızın amacı, mevcut ulaşım ve araç ekosisteminin reddedilemezlik ve mutabakat sağlama güvenlik gereksinimleri karşılamayı sağlayacak, aynı zamanda akıllı ulaşım ve bağlantılı araç IoT ekosistemlerinin gelişimini destekleyecek, Blockchain teknolojisine dayalı bir güvenli veri yönetim modeli ortaya koymaktır. Önerilen modelde, IoT sistemlerinin kısıtlarını göz önünde bulunduran ve akıllı ulaşım endüstrisindeki gelişmelere bağlı olarak, yeni nesil akıllı araç kitleri ile entegre çalışabilen güvenli, etkin ve yenilikçi bir altyapı sağlanacaktır.

A Blockchain Based Data Management Model

ARTICLE INFO

Received: 04.11.2019
Accepted: 23.12.2019

Keywords:
Blockchain, IoT, Smart Transportation, Connected Car

Corresponding Authors
e-mail:
busraozdenizci@gtu.edu.tr

ABSTRACT

Internet of Things (IoT) enables objects to gain capabilities such as sensing, vision and warning and to communicate with each other. With the development of smart device resources and communication network capabilities, a variety of smart environments - health, grid, home, factory, agriculture, city, car, transport and so on- are rapidly evolving. In this context, security and privacy of IoT data to be processed and operations to be performed is an important issue. The aim of our research is to provide a secure data management model based on Blockchain technology which ensures non-repudiation and consensus security requirements of current transportation ecosystem, as well as supports development of smart transportation and connected car ecosystems. In accordance with recent developments in smart transportation industry, proposed model will provide a secure, efficient and innovative infrastructure that takes into account IoT systems limitations and is able operate with new generation of smart car kits.

1. *GİRİŞ (INTRODUCTION)*

Günümüzde içinde bulunduğumuz Endüstri 4.0 dönemi ile makineleşme, otomasyon sistemleri, yeni iletişim ve ağ teknolojileri, makineler arası iletişim (M2M) ve -makinelerin ötesinde- iletişim kurabilen nesnelerin iletişimi, nesneler arası iletişimin oluşturduğu verilerin yönetimi kavramları giderek büyük önem kazanmaktadır. Özellikle iletişim ağ teknolojilerinin gelişimi ile beraber algılama, görme, uyarma, tetikleme ve benzeri işlevselliklerin, fiziksel nesnelere yetenek olarak kazandırılması sağlanmıştır. Birbiri ile iletişim kurabilen "akıllı" nesneler (smart things, smart objects) sayesinde üretkenlik kazandıran, zaman ve maliyet verimliliği sağlayan, daha az insan müdahalesi gerektiren ve yaşam kalitesini artıran hizmetlerin geliştirilmesi ve çeşitli "akıllı" ortamların (smart environments) yaratılması mümkün olmuştur. Tüm bu gelişmeler, Nesnelerin İnterneti (Internet of Things, IoT) olarak adlandırılan geniş ve entegre bir ekosistemi oluşturmuştur.

IoT, gerçek dünya nesnelerine algılama, uyarma, tetikleme ve benzeri yeteneklerin kazandırılarak, insan müdahalesi olmadan "akıllı" nesnelerin kendi aralarında iletişim kurmasını sağlayan bir dizi teknolojiyi kapsar [1, 2]. IoT yaklaşımı, fiziksel nesnelerin kendi aralarında ve hatta İnternet üzerinden diğer cihazlarla veya servislerle, her zaman ve her yerde iletişim kurmasını sağlayacak tanımlama, algılama, uyarma, ağ oluşturma ve veri işleme yeteneklerine sahip bir kavram olarak tanımlanmaktadır [3, 4, 5].

Akıllı nesneler sahip oldukları yetenekler sayesinde, çeşitli heterojen kaynaklardan bilgi toplama, paylaşma, işleme ve benzeri bilgi yönetimi işlemlerini yapabilmektedir. Elde edilen veriler üzerinde veri analitiği ve makine öğrenmesi çalışmalarının yaygınlaşmasıyla katma değerli ve yenilikçi servislerin sunulması sağlanabilmektedir. Bu sayede geniş bir uygulama portföyüne olanak sağlayan IoT sistemleri; akıllı sağlık, akıllı şebeke, akıllı şehir, akıllı ev, akıllı tarım, akıllı ulaşım, akıllı araç ve benzeri birçok alanda hızla yayılmaktadır [2, 5, 6].

Son yıllardaki gelişmelere bağlı olarak, IoT alanında akıllı ulaşım (smart transportation) kapsamında bağlantılı araç (connected car) ve güvenlik konusu büyük bir hızla önem kazanmaktadır. Akıllı araç kiti ve benzeri gelişmiş geçit cihazlar (gateway) ile araçlarda bulunan çeşitli algılayıcılardan (sensors) veriler –örneğin motor sıcaklığının yükselmesi, akü voltajının düşmesi ve benzeri veriler- toplanarak kullanıcı sürüş deneyiminin zenginleştirilmesi hedeflenmektedir [7]. Akıllı ve bağlantılı araç altyapılarının giderek geliştirilmesi, kullanıcı deneyimi ve araç performansı verimliliğini iyileştirmekle beraber yenilikçi hizmetlerin geliştirilmesini de sağlayabilir.

Günümüzde, hızla gelişen IoT vizyonu diğer taraftan güvenlik kapsamında zorlu sorunlarla da karşı karşıyadır. IoT sistemlerin heterojenlik ve büyük ölçekli ağlar sağlaması, IoT güvenliğini geleneksel ağ güvenlik sorunlarından ayıran ana faktörlerdir. IoT cihazlarının hem depolama hem de hesaplamada sınırlı yeteneklere sahip olması bu alandaki önemli sorunlardan biridir; IoT cihazları yoğun hesaplama kaynakları gerektiren kriptografi gibi karmaşık işlemleri gerçekleştirmek için yeterince güçlü değildir [2, 8, 9].

Özellikle, akıllı ortamlarda gerçekleşen kullanıcı etkinliklerinin izlenmesi ve hassas verilerin toplanması, -yaşam kalitesini arttıran çeşitli acil durum, ilk yardım, sağlık, yangın ve benzeri servislerin sağlaması için gerekli olurken- verilerin gizliliği ve güvenliği konularını beraberinde getirmektedir. Örneğin, aracın kullanımı esnasında güvenli bir şekilde doğru bilgiyi alabilmek ulaşım ekosistemindeki bulunan tüm paydaşlar için önemli bir konudur. Bir trafik kazası anında araç hızının veya emniyet kemeri kullanım bilgisinin tespit edilmesi, inkâr edememe (non-repudiation) gereksiniminin karşılanması, sorumların tespitinin sağlıklı yapılması ve benzeri süreçlerdeki işlemlerin kayıt altına alınması gerekmektedir. Böylece bir aracın karıştığı kaza sonrasında sürücü aşırı hız yaptığı bilgisinin bilinirliğini önleyemez. Bu noktada, Blockchain (Blok zinciri) teknolojisi geniş ve karmaşık içerikli akıllı ortamlar için güvenli bir veri yönetim modeli sunabilecek özelliklere sahiptir.

Son yıllarda giderek önem kazanan Blockchain teknolojisi, bilgi ya da olayları (gerçekleri) gerçekleştiği zaman bilgisi (timestamp) ile birlikte sonradan değiştirilemez şekilde kayıt altına almayı mümkün kılan önemli bir güvenlik bir teknolojisidir [8]. Dağıtık bir veri ağı üzerinde faaliyet gösterme olanağı sunan Blockchain teknolojisi, verileri güvenli ve kalıcı olarak saklama, hızlı transfer etme ve erişilebilir olma ve benzeri avantajlara sahiptir. Blockchain, birbirine güvenmeyen kullanıcıların üçüncü bir tarafa ihtiyaç duymaksızın değişmez bir veri üzerinde anlaşabilmelerini sağlar. Bu kapsamda, IoT içerikli ortamlarda üretilen verilerin Blockchain teknolojisi ile kayıt altına alınması neticesinde yenilikçi hizmetlerin sunulması sağlanabilir.

Günümüzde mevcut ulaşım ve araç ekosistemlerindeki paydaşların; araç satış firmaları, araç kiralama firmaları, araç onarım firmaları, sigorta firmaları, araç takip firmaları, kamu kurumları ve

benzeri paydaşların birbirlerine güvenmedikleri için her biri kendi veri sistemini yönetmekte; dolayısı ile diğer paydaşların verilerinden istifade edilememektedir. Böyle durumlarda, veri bütünlüğü ve inkâr edilememe kapsamında yüksek güvenlik seviyesi sağlanamamaktadır. Mevcut ulaşım ve araç ekosistemindeki olan problemler iki ana grupta incelenebilir: Paydaşların her birinin kendi veri sistemini kullanması nedeni ile veri bütünlüğünün sağlanmaması problemi ve mutabakat sağlanmaması kapsamındaki problemler. Kaza durumlarında veya kaza durumu dışındaki sigorta işlemlerinde sahte bilgilerin oluşturulabilmesi, trafik ve ulaşım ekosisteminde bulunan paydaşlar arasında güvensizlik ve tutarsız bilgilerin oluşması, paydaşların her birinin ayrı bir bilgi sistemi kullanması dolayısı ile oluşan bilgi eksikliği ve bilgi tutarsızlığı oluşması, hatalı bilgi kullanması mutabakat sağlanmaması kapsamındaki problemlere örnek verilebilir.

Çalışmamızın amacı, ulaşım ve araç ekosisteminde bahsedilen problemleri çözümleyecek Blockchain teknolojisine dayalı bir güvenli veri yönetim modeli ortaya koymaktır. Geliştirilmesi hedeflenen model, IoT sistemlerinin kısıtlarını göz önünde bulunduran ve akıllı ulaşım sektöründeki gelişmelere bağlı olarak, yeni nesil akıllı araç kitleri ile entegre çalışabilen ve bağlantılı araçların gelişimini destekleyebilecek güvenli, etkin ve yenilikçi bir altyapıya sahip olacaktır.

2. *YÖNTEM* *(METHODOLOGY)*

Çalışmamız kapsamında, betimsel araştırma yaklaşımı izlenerek, bulgular bölümünde araştırma sonuçları ile önerilen modelimizin ön detayları paylaşılmaktadır. Literatür taraması kapsamında, ilgili araştırma problemini adresleyen konuların, çeşitli elektronik veri tabanlarında (IEEE Digital Library, ACM Portal, Science Direct ve benzeri) taraması gerçekleştirilmiştir.

Araştırma konusu oldukça yeni bir alanı adreslemektedir. Blockchain teknolojisinin, akıllı ulaşım ve bağlantılı araçlar gibi geniş ve karmaşık IoT sistemlerinde gerekli olan inkâr edilememe ve mutabakat sağlama güvenlik unsurlarına potansiyel bir çözüm olabileceği öngörülmektedir. Blockchain teknolojisi ile kayıt altına alınmış olan bir gerçek, kayıt sonrasında konu ile ilişkili bir paydaş tarafından reddedilme çabası olsa dahi -Blockchain teknolojisinin dayandığı matematiksel olarak ispat edilebilir içeriği nedeni ile- inkâr edilememektedir.

Literatür taramasıyla, ulaşım ve araç ekosistemleri için önereceğimiz Blockchain tabanlı güvenli veri yönetim modeli bileşenleri, bileşenlerin özellikleri belirlenmiştir ve önerilen modelin ön hazırlık çalışmaları paylaşılmıştır.

3. *BULGULAR* *(FINDINGS)*

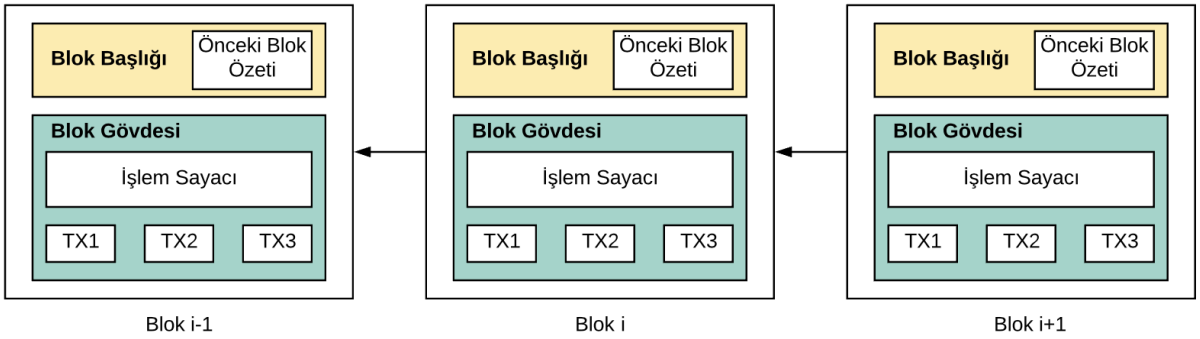
3.1. Blockchain ve IoT *(Blockchain and IoT)*

Blockchain teknolojisi, 2008'de Satoshi Nakamoto tarafından yayınlanan makalesinde Bitcoin kripto para sistemiyle beraber ortaya çıkmaktadır [10, 11]. Blockchain, kriptografik hash fonksiyonları kullanarak birbirine bağlanmış blokların bir listesidir. Bu blokların her biri, finansal işlemler gibi belirli işlemlerle ilgili bilgileri içeren bir "container" olarak tanımlanabilir. Yeni işlemler oluşturuldukça liste sürekli büyümeye devam eder ve işlemler, ağa bağlı düğümler (node) adı verilen varlıklar tarafından yaratılır. Bir işlem belirli bir düğüm tarafından oluşturulduktan sonra, işlemler kabul edilmeden ve bloğa eklenmeden önce doğrulanmak üzere tüm ağa yayınlanır [12].

Şekil 1'de gösterildiği üzere, ana bloğun (parent block) hash değeri kullanılarak, blokların birlikte zincirlendiği bir Blockchain örneğini göstermektedir. Her blok bir başlık ve gövdeden oluşur. Ana Blok Hash değerine ek olarak, blok başlığında blok versiyonu, zaman damgası, nonce ve diğerleri gibi başka alanlar da vardır. Blok gövdesi, işlem sayısını ve işlemlerin kendisini gösteren bir sayaç içerir.

Blockchain, iki veya daha fazla taraf arasındaki işlemleri etkin ve doğrulanabilir, kurcalamaya karşı dirençli (tamper-resistance) ve kalıcı bir şekilde kaydeden herkese açık bir defter olarak tanımlanabilir [12]. Blockchain, güvenlik seviyesi az kullanıcıların, üçüncü taraflara ihtiyaç duymaksızın değişmez bir veri üzerinde anlaşabilmelerini sağlar. Bu özellikler, Blockchain teknolojisinin finans ve IoT alanlarında yoğun ilgi görmesini sağlamaktadır.

IoT sistemleri, milyarlarca heterojen cihazı birbirine bağlayabilmesine ve zengin uygulamalara imkân sağlaması diğer taraftan bazı açık konuları da beraberinde getirmektedir. Heterojenlik ve büyük ölçekli nesneler ile kullanılan ağ protokolleri, IoT güvenliğini geleneksel ağların güvenlik sorunlarından ayıran ana faktörlerdir. Birçok çalışmada IoT'nin güvenlik, gizlilik ve ölçeklenebilirlik konuları incelenmiştir [13-17].



Şekil 1. Blockchain Yapısı
(Structure of Blockchain)

Yapılan çalışmalarda akıllı ev, akıllı şehir ve akıllı sağlık kapsamında kullanıcıların hareketleri, etkileşimleri ve alışkanlıkları ile ilgili hassas kişisel bilgilerin korunması gerektiği vurgulanmaktadır. IoT güvenliği konusunda yapılan diğer bir çalışmada [18], ana güvenlik konularının Nesne Tanımlaması, Kimlik Doğrulama ve Yetkilendirme, Gizlilik, Hafif Kriptosistemleri ve Güvenlik Protokolleri, Yazılım Güvenlik Açığı ve IoT Kötü Amaçlı Yazılım olduğunu belirtilmiştir.

Blockchain teknolojisinin, IoT sistemlerinde bahsedilen güvenlik ve gizlilik sorunlarını çözme potansiyeline sahip olduğu incelenmiştir. Literatürde, IoT'de Blockchain teknolojisini benimseme yeteneğini araştıran bazı önemli çalışmalar bulunmaktadır. Kshetri [19] çalışmasında, Blockchain teknolojisinin özellikle kimlik ve erişim yönetimi kapsamında IoT sistemlerini güçlendirebileceği konusunda bir model sunmaktadır. Dorri ve arkadaşları [20] çalışmasında, Blockchain-IoT entegrasyonunu optimizasyonunu sağlamayı hedefleyen, akıllı ev ortamlarında kullanılabilecek bir Blockchain çözümü sunmaktadır. Blok doğrulama işlem zamanını azaltmaya dayanan az maliyetli, etkili, güvenli ve hafif bir model ortaya koymuştur.

3.2. Önerilen Model *(Proposed Model)*

Geliştirilecek olan Blockchain tabanlı güvenli araç veri yönetim modeli ile araç ekosisteminde için bahsedilen problemlerin Blockchain teknolojisi kullanılarak çözümlenmesi hedeflenmektedir. Blockchain teknolojisinin özellikleri sayesinde, merkezi bir otoriteye ihtiyaç duymadan işlemlerin güncel, gerçek zamanlı ve tutarlı olarak oluşturulması mümkündür. Böylece, araç kullanım yaşam döngüsü boyunca araca ve sürücüye dair reddedilemez şekilde güvenli kayıtların oluşturulması sağlanacaktır. Veri bütünlüğü ve mutabakata bağlı problemlerin çözümlenerek, sağlıklı ve güvenli bir araç bilgi sistemi oluşturulacaktır.

Geliştirilmesi planlanan modelde, Blockchain ağı şu düğümlerden oluşmaktadır:

- Kullanıcılar: Blockchain tabanlı araç bilgi yönetim sistemine kayıt olmuş araç sahibi kullanıcılardır. Kullanıcılara ait kişisel bilgiler ve sahip oldukları araçlar hakkındaki bilgiler Blockchain ağına aktarılır.
- Araç Kiti Merkezi: Akıllı araç kitleriyle elde edilecek olan veriler bu modelin diğer önemli bir kısmını oluşturacaktır. Araç kiti bağlı olduğu araç hakkında, Blockchain ağına şu bilgileri aktaracaktır: Aracın GPS (konum) bilgileri, Seyahat başlangıcı (içinde başlangıç GPS bilgileri ile birlikte), Seyahat bitişi (içinde bitiş GPS bilgileri ile birlikte), Seyahatin başlangıç ve bitiş saati, Seyahatin başlangıç ve bitişindeki GPS paketleri, Maksimum hız ve benzeri bilgiler.
- Sigorta Firmaları: Araçları sigortalayan, olası bir kaza sonrasında ise devreye giren ve zararı tazmin eden firmalardır. Bu aktör, sigortalanan araçların poliçe detaylarına ve sigorta poliçesi kullanımına ait bilgileri Blockchain ağına aktarır.
- Araç Kiralama Firmaları: Akıllı araç kiti entegre edilmiş araçları kiralayan firmalar, kiraladıkları araçları ve kullanıcılarına dair bilgileri Blockchain ağına aktarır.
- Araç Onarım Merkezleri: Herhangi bir kaza durumunda, müdahale etmesi ve aracın teknik problemini çözümlemesi gereken aktördür. Bu aktör, araç ile ilgili sorunlarının çözüm sürecine dair bilgileri Blockchain ağına aktarır.
- Diğer Aktörler: sistem içinde bulunan ve gerektiği durumlarda sisteme dâhil olan Tüketici Organizasyonları, Emniyet Müdürlüğü, Trafik Polisleri, Hastane ve Benzin İstasyonu ve benzeri aktörler de birer düğüm olarak Blockchain ağına katılabilir.

Blockchain tabanlı araç veri yönetim sisteminin öncelikli hedefi; ekosistemdeki tüm paydaşlar

(düğümler) için, yüksek derecede güvenli ve inkâr edilemez kayıt bilgileri kullanılarak mutabakat sağlanmasıdır. Aracın kullanılması ile başlayan tüm işlemlerde aktörler arasındaki her türlü mutabakat gerektiren işlem, Blockchain özellikleri kullanılarak sağlayacaktır. Merkezi bir otorite olmadan yapılacak olan her işlem (transaction) kaydı, paydaşların %51'inin onayının sağlandığı takdirde, Blockchain ağına bir daha değiştirilmemek üzere eklenecek ve mutabakat altyapısı bu şekilde sağlanacaktır.

Güvenli mutabakat sağlanması için Blockchain teknolojisinin en önemli özelliklerinden biri olan Smart Contract kullanılacaktır. Smart Contract modelleri, Blockchain ağını kullanarak iki parti arasındaki anlaşmaları kolaylaştırma, yürürlüğe koyma ve yürütme yeteneğine sahiptir. Önerilen sistem kapsamındaki paydaşlardan gelen talepler, Smart Contract ile yönetilecektir. gereksinimlerini karşılaşmak amacıyla, Blockchain teknolojisine dayanan güvenli bir veri yönetim modeli sunulmaktadır. Önerilen modele ait geliştirilmesi planlanan Blockchain ağının gereksinimleri ön hazırlık çalışmalarıyla paylaşılmaktadır.

Aynı zamanda, akıllı araç kitleri ile entegre çalışacak olan Blockchain tabanlı araç bilgi yönetim sistemi, gerçek zamanlı ve güvenilir verilerin elde edilerek, geniş ve entegre bağlantılı araç ekosisteminde yer alan ve birbirine güvenmeyen paydaşlara etkin, güvenli ve insan müdahalesi gerektirmeyen bir veri yönetim ve iletişim platformu sunacaktır. Araştırma-geliştirme açısından önemli bulgular edineceğimiz bu çalışmanın devamında, Blockchain ağında kullanılan madencilik tekniklerinin incelenmesini, güvenlik ve algoritma tasarımlarının incelenecektir.

Geliştirilmesi planlanan yenilikçi güvenli veri yönetim modeli, hatta ve Milli Otomobil geliştirilmesi konusundaki çalışmaların bilişim ağırlıklı teknolojik yönünü desteklemesi mümkün olacaktır ve hatta geniş, ölçeklenebilir, birlikte çalışabilen ve sürdürülebilir diğer akıllı ortamların geliştirilmesini sağlaması öngörülmektedir.

4. *SONUÇ* *(CONCLUSION)*

Bu çalışmada, ulaşım ve araç ekosistemlerinde -inkâr edememe ve mutabakat sağlama- güvenlik gereksinimlerini karşılaşmak amacıyla, Blockchain teknolojisine dayanan güvenli bir veri yönetim modeli sunulmaktadır. Önerilen modele ait geliştirilmesi planlanan Blockchain ağının gereksinimleri ön hazırlık çalışmalarıyla paylaşılmaktadır.

Aynı zamanda, akıllı araç kitleri ile entegre çalışacak olan Blockchain tabanlı araç bilgi yönetim sistemi, gerçek zamanlı ve güvenilir verilerin elde edilerek, geniş ve entegre bağlantılı araç ekosisteminde yer alan ve birbirine güvenmeyen paydaşlara etkin, güvenli ve insan müdahalesi gerektirmeyen bir veri yönetim ve iletişim platformu sunacaktır. Araştırma-geliştirme açısından önemli bulgular edineceğimiz bu çalışmanın devamında, Blockchain ağında kullanılan madencilik tekniklerinin incelenmesini, güvenlik ve algoritma tasarımlarının incelenecektir.

Geliştirilmesi planlanan yenilikçi güvenli veri yönetim modeli, hatta ve Milli Otomobil geliştirilmesi konusundaki çalışmaların bilişim ağırlıklı teknolojik yönünü desteklemesi mümkün olacaktır ve hatta geniş, ölçeklenebilir, birlikte çalışabilen ve sürdürülebilir diğer akıllı ortamların geliştirilmesini sağlaması öngörülmektedir.

KAYNAKLAR *(REFERENCES)*

[1] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends". *Information Systems Frontiers*, pp. 17: 261, 2015. Doi: 10.1007/s10796-014-9489-2.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications." *IEEE Communications Surveys & Tutorials*, 17.4, pp. 2347-2376, 2015. Doi: 10.1109/COMST.2015.2444095.

[3] O. J. A. Pinno, A. R. A. Gregio, and L.C. De Bona, "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT", in *IEEE Global Communications Conference*, 2017, pp. 1-6.

[4] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", *Journal of Information Security and Applications*, 38, pp. 8-27, 2018. Doi: https://doi.org/10.1016/j.jisa.2017.11.002.

[5] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using Blockchain platform", in *19th IEEE International Conference on Advanced Communication Technology* (ICACT), 2017, pp. 464-467.

[6] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things", *Security and Communication Networks*, 9(18), pp. 5943-5964, 2016. Doi: https://doi.org/10.1002/sec.1748.

[7] Turkcell, Kopilot. Available: https://www.turkcell.com.tr/servisler/kopilot [Accessed: 12 Kasım 2019].

[8] J. Lin, et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. " *IEEE Internet of Things Journal*, 4(5), pp. 1125-1142, 2017. Doi: 10.1109/JIOT.2017.2683200.

[9] R. Khan, S. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet Of Things Architecture, Possible Applications and Key Challenges", in *10th IEEE International Conference on Frontiers of Information Technology (FIT)*, 2012, pp. 257-260.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008.

[11] L. Iuon-Chang, and T. Liao, "A Survey of Blockchain Security Issues and Challenges", *IJ Network Security*, 19(5), pp. 653-659, 2017. Doi: 10.6633/IJNS.201709.19(5).01.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", in *IEEE International Congress on Big Data*, 2017, pp. 557-564.

[13] B. N. Silva, M. Khan, and K. Han, "Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges", *IETE Technical Review*, 35(2), pp. 205-220, 2018. Doi: https://doi.org/10.1080/02564602.2016.1276416.

[14] S. Hameed, et al. "Understanding security requirements and challenges in Internet of Things (IoT): A review", *Journal of Computer Networks and Communications*, 2019. Doi: https://doi.org/10.1155/2019/9629381.

[15] V. Gazis, et al. "Short paper: IoT: Challenges, projects, architectures." in *Proceedings of 18th IEEE International Conference on Intelligence in Next Generation Networks*, 2015, pp. 145-147.

[16] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services", in *IEEE world forum on Internet of Things (WF-IoT)*, 2014, pp. 287-292.

[17] S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A Survey", *Information Systems Frontiers*, 17(2), pp. 243-259, 2015. Doi: 10.1007/s10796-014-9492-7.

[18] Z. K. Zhang, et al., "IoT Security: Ongoing Challenges and Research Opportunities," in *IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 230-234.

[19] N. Kshetri, "Can blockchain strengthen the internet of things? " *IT Professional*, 19(4), pp. 68-72, 2017. Doi: 10.1109/MITP.2017.3051335.

[20] A. Dorri, S. Kanhere and R. Jurdak, "Towards an optimized blockchain for IoT. " in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, ACM, 2017, pp. 173-178.