T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DOKTORA TEZİ

ARAÇLAR ARASI HABERLEŞMEDE GÜVENLİ MODEL GELİŞTİRİLMESİ

Şükrü OKUL

DANIŞMAN
Dr. Öğr. Üyesi Fatih KELEŞ

II. DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği, Doktora Programı

Mayıs, 2024

TEZ KABUL VE ONAYI

Şükrü OKUL tarafından, **Dr. Öğr. Üyesi Fatih KELEŞ** danışmanlığında hazırlanan **"Araçlar Arası Haberleşmede Güvenli Model Geliştirilmesi"** başlıklı bu çalışma, jürimiz tarafından **27/05/2024** tarihinde yapılan sınav sonucunda **oy birliği** ile başarılı bulunarak **Doktora Tezi** olarak kabul edilmiştir.

Tez Jürisi

		İmza	Sonuç
DANIŞMAN	Dr. Öğr. Üyesi Fatih KELEŞ İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Prof. Dr. Ahmet SERTBAŞ İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Doç. Dr. Şerif BAHTİYAR İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Doç. Dr. Atakan KURT İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Dr. Öğr. Üyesi Erkan USLU Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret

Bu çalışmamı eğitim hayatım boyunca bana destek olan annem Havva OKUL, babam Ahmet Emin OKUL, eşim Ayşegül OKUL, kardeşim Şeyma BAYRAKTAR'a, hayatımı neşelendiren kızım Amine Zümra OKUL, ikizlerim Ahmet OKUL ve Mustafa OKUL'a ithaf ediyor ve hepsine sevgilerimi sunuyorum.

BÜTÇE DESTEKLERİ

Araçlar Arası Haberleşmede Güvenli Model Geliştirilmesi

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.

TEŞEKKÜR

Tüm eğitim öğretim hayatım boyunca bana tek bir harf bile öğreten tüm hocalarıma ve Doktora hayatım boyunca her konuda bana yardımcı olan Sayın Fatih KELEŞ ve Muhammed Ali AYDIN hocalarıma çok teşekkür ediyorum. Ayrıca Tez İzleme Komitesi sürecinde de sundukları katkılardan dolayı Sayın Ahmet SERTBAŞ ve Şerif BAHTİYAR hocalarıma da çok teşekkür ediyorum.

Mayıs 2024 Şükrü OKUL

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

μ : nü
β : beta
π : pi
α : alfa
ɣ : lambda

Kısaltmalar **Açıklama**

ALPR : Otomatik Plaka Okuyucuları
BC : BlockChain
BZ : Blok Zincir
BGP : Sınır Geçidi Protokolü
CA : Merkezi Otorite
CTS : Göndermeyi Temizle
DAO : Merkezi Olmayan Otonom Organizasyon
DSRC : Özel Kısa Menzilli İletişim
EMT : Acil Durum Mesaj İletimi
GPS : Global Positioning System
GMT : General Message Transportation
IoV : Araçların İnterneti
IoT : Nesnelerin İnterneti
ITS : Intelligent Transportation System
İSS : İnternet Servis Sağlayıcısı
LİDAR : Lazer Işıklı Algılama ve Menzil
LSB : Hafif Ölçeklenebilir Blok Zinciri
PK : Ortak Anahtar
PKI : Ortak Anahtar Altyapısı
PoA : Otorite Kanıtı
PoW : İş Kanıtı

PoS : Varlık Kanıtı
RSU : Yol Kenarı Birimi
RTS : Gönderme İsteği
SDR : Standard Delay Requirements
TPS : Transaction Per Second
VANET : Vehicular Ad Hoc Network
VSN : Araç Sosyal Ağı
V2I : Araç-Altyapı
V2V : Araç-Araç

ÖZET

DOKTORA TEZİ

ARAÇLAR ARASI HABERLEŞMEDE GÜVENLİ MODEL GELİŞTİRİLMESİ

Şükrü OKUL

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği, Doktora Programı

Danışman : Dr. Öğr. Üyesi Fatih KELEŞ

II. Danışman : Doç. Dr. Muhammed Ali AYDIN

Bu çalışmada günümüzde önemi her geçen gün artan araçlar arası haberleşmede güvenli bir model önerilmektedir. Önerilen modelde güvenliği arttırmak ve güncel bir teknoloji kullanmak amacıyla blok zincir teknolojisi kullanılmaktadır. Ayrıca performansı ve güvenliği birlikte düşünerek konsorsiyum blok zincir kullanılmaktadır. Bu model önerilirken giriş kısmında çalışmanın amacı ve detaylarından, kavramsal çerçeve kısmında ise VANET teknolojisi, blok zincir teknolojisi ve daha önce yapılan çalışmalar hakkında bilgi verilmektedir. Daha sonra araçlar arası iletişimde mesajlaşma süreci ile ilgili güncel çalışmalar incelenmiş, avantajları ve dezavantajları hakkında bilgi verilmektedir. Bu bilgilerden sonra yöntem başlığında önerilen sistem tasarımı detaylı olarak anlatılmaktadır. Ek olarak yöntem başlığında yine blok zincir teknolojisi kullanılarak tasarladığımız araç sosyal ağından bahsedilmektedir. Sistem tasarımında bahsettiğimiz uygulamamızın test sonuçları bulgular kısmında irdelenerek teorik olması gereken sonuçlar ile karşılaştırılmaktadır. Karşılaştırma yapılırken daha önce fark edilmemiş bir bakış açısıyla incelenmektedir. Kuyruk kısmında ise gerçek zamanlı olarak oluşabilecek ihtimaller göz önünde bulundurularak çalışma yapılmış ve aynı anda blok zinciri üzerinden isteklerin alınması ve bunların değerlendirilerek bir işlem ile blok oluşturulması

süreci dikkate alınmaktadır. Tüm bu süreçlerde güvenlik dışında mobilitesi yüksek bir sistem olduğu için performans ile ilgili çalışmalar ve sonuçlarda irdelenmektedir. Sonuçları irdelemeden önce teorik olarak tüm bu sistem süreçlerinde olması gereken performans verileri hesaplanmaktadır. Hesaplanan değerler ile elde edilen sonuçların sonuçları karşılaştırılmaktadır. Ayrıca diğer çalışmalarla ilgili olarak teorik ve performans bazında karşılaştırma yapılmaktadır. Sonuç bölümünde son değerlendirme yapılarak, çalışma ile ilgili bilgiler sonuçlandırılmaktadır.

Mayıs 2024 , 70 sayfa.

Anahtar kelimeler: Blok Zincir, VANET, Güvenlik

ABSTRACT

Ph.D. THESIS

DEVELOPING A SAFE MODEL IN INTER VEHICLE COMMUNICATION

Şükrü OKUL

İstanbul University-Cerrahpaşa

Institute of Graduate Studies

Department of Computer Engineering

Computer Engineering, Ph.D. Program

Supervisor : Assist. Prof. Dr. Fatih KELEŞ

Co-Supervisor: Assoc. Prof. Dr. Muhammed Ali AYDIN

In this study, a secure model is proposed for inter-vehicle communication, the importance of which is increasing day by day. In the proposed model, blockchain technology is used to increase security and use an up-to-date technology. In addition, consortium blockchain is used by considering performance and security together. While this model is recommended, information is given about the purpose and details of the study in the introduction, and information about VANET technology, blockchain technology and previous studies in the conceptual framework. Then, current studies on the messaging process in inter-vehicle communication were examined and information was given about its advantages and disadvantages. After this information, the proposed system design is explained in detail in the method title. In addition, in the method title, the vehicle social network that we designed using blockchain technology is mentioned. The test results of our application, which we mentioned in the system design, are examined in the findings section and compared with the results that should be theoretical. It is examined from a perspective that has not been noticed before while making comparisons. In the queue part, the study was carried out by taking into account the

possibilities that may occur in real time, and the process of simultaneously receiving requests over the block chain and evaluating them and creating a block with a transaction is taken into account. In all these processes, since it is a system with high mobility apart from security, it is examined in studies and results related to performance. Before examining the results, the performance data that should theoretically be in all these system processes are calculated. The calculated values and the results of the obtained results are compared. In addition, comparisons are made with other studies on a theoretical and performance basis. In the conclusion part, the final evaluation is made and the information about the study is concluded.

May 2024, 70 pages.

Keywords: Blockchain, VANET, Security

1. GİRİŞ

Araçlar arası iletişim her geçen gün daha önemli hale gelmektedir. Aynı zamanda Araçtan Araca İletişimin birçok avantajı ve dezavantajı vardır. Birçok çalışmada çeşitli teknolojiler bu iletişime entegre edilmeye çalışılmaktadır. Bu teknolojilerin en günceli blok zincir teknolojisidir.

Blok zincir teknolojisi son zamanlarda ulusal ve uluslararası basın, çeşitli uluslararası kuruluşlar, özel sektör ve kamu kurumları tarafından büyük ilgi görmesine rağmen bazı araştırmacılar tarafından potansiyel olarak internetten daha güçlü bir teknoloji olarak ifade edilmektedir [1]. Akademik açıdan bakıldığında, kısa bir süre önce literatürde blok zincir ile ilgili bir çalışmaya rastlamak çok zor iken, bu konuda çok sayıda çalışmanın olduğu ve giderek sayılarının arttığı görülmektedir [2].

Blok zincir ile ilgili çalışmalar pek çok alanda yapılmakta ve pek çok araştırmacının bu konuya odaklanması sayesinde pek çok çalışma bulunmaktadır. Nesnelerin İnterneti, akıllı havaalanları, akıllı tıp veya güvenlik, merkezi olmayan yönetim gibi diğer mobil hizmetlerle iş birliği yaparak blok zincir tabanlı sistemlerin etkinliğini, kullanılabilirliğini ve güvenilirliğini artırmak bunlardan bazılarıdır [3-8]. Kaynak doğrulama [9], güven ve itibar yönetimi [10], olay ve mesaj alışverişi yönetimi [11], akıllı ödeme kullanımı [12], trafik denetimi [13] güvenliği sağlamak için benzer avantajlar elde etmek için kullanılan alanlardan bazılarıdır.

Araçlar arası haberleşmede olduğu gibi internet bağlantısı bulunan araçlarda da blok zincir teknolojisi kullanılmaktadır. Mevcut sistemlerde IoV'nin (Araçların İnterneti) gerçekliğini sağlamak için çeşitli kimlik doğrulama yöntemleri öneren bazı çalışmalar vardır. Bazılarında kimlik doğrulama için blok zincir kullanan IoV'lerin kimliğini doğrulamak için önerilen bir Sertifika Yetkilisi (CA) vardır, bu CA aslında merkezi bir organdır. Başka bir deyişle, bu güvenilir bir otoritenin varlığının bir göstergesidir. Örneğin, Lai, blok zincir teknolojisini, blokları kullanarak kimlik doğrulama sürecinin etkinliğini artırmak ve yönlendirici kontrol veritabanları arasında bilgi paylaşmak için bir çalışma sunmaktadır [14]. Başka bir çalışmada Javaid, CA yani merkezi otoriteyi kullanarak kimlik doğrulaması yapmakta ve blok zincir teknolojisini kullanarak kimlik doğrulama bilgilerini orada depolamakta ancak sisteme getirilen

ek yüklerden burada bahsetmemektedir [15]. Başka bir çalışmada, akıllı bir ödeme sistemi geliştirmek için sadece araçlar değil, aynı zamanda altyapının güven bilgileri de bir blok zincirinde saklanmakta ve herhangi bir işlemden önce hem kasiyer hem de sürücü birbirinin orijinalliği ve güvenilirliği açısından kontrol edilmektedir. İşlem bilgileri de blok zincirinde saklanmaktadır [12]. Ali, çalışmasında yetkili ve yetkisiz araç bilgilerini ayrı ayrı depolamak için birkaç blok zincir kullanılmaktadır [16]. Ayrıca Ali, sertifika tabanlı sistemin ek yükünü ortadan kaldırmak için sertifikasız bir kimlik doğrulama protokolü önermektedir. Bu çalışmaya benzer diğer iki çalışmada, biri sertifikalı ve iptal edilmiş araçların bilgilerini depolamak için kullanılırken, diğeri araçlar arasındaki iletişimden kaynaklanan mesajları depolamak için kullanılan iki farklı blok zinciri kullanılmaktadır [17-18]. Öte yandan Zhang, blok zincir teknolojisini, kimlik doğrulama bilgileri, konum ve yön bilgileri ile birlikte blok zincir tabanlı bir depolama sisteminde depolar ve ayrıca itibar bilgilerini depolamak için tüm kural ihlallerini blok zincir'e eklemektedir [19]. Sertifika oluşturma, imzalama ve doğrulama yüksek ek yük getirdiğinden, kimlik doğrulama bilgilerinin saklanması ve blok zincir araçlarının gizliliğinin korunması başka bir çalışmada kullanılmaktadır [20]. Ancak bu avantajı sağlayan bu çalışmada güvenlik hizmetlerini artırma yöntemi yüksek bir hesaplama yükü oluşturmaktadır. Benzer şekilde, diğer bazı çalışmalarda, birçok protokol, kimlik doğrulama işlemlerini tamamlamak için çok fazla zaman ve hesaplama yükü gerektirmektedir [21-25]. Ayrıca, Li ve diğerleri, Salem ve diğerleri tarafından önerilen bir yöntem araçların kimlik doğrulama bilgilerini depolamak için çok fazla depolama alanı gerektirmektedir [26-27].

Tüm bu durumlar göz önünde bulundurulduğunda önerdiğimiz sistemde güvenliği blok zincir teknolojisi ile sağlanmaktadır. Aynı zamanda depolama alanı ve performans gibi gerekçeleri de düşünerek modelimizde konsorsiyum blok zinciri hafif bir şifreleme algoritması ile kullanarak bu konulardaki ihtiyaçları da karşılanmaktadır.

1.1. PROBLEM TANIMI

Çalışmada dört temel problem için çözüm sunulmaktadır. Bu problemler merkezi sistemlerdeki bağımlılıkların ortaya koyduğu problemler, mobilitesi yüksek sistemlerdeki haberleşmenin zorluğu, veri bütünlüğünün sağlanması ve mahremiyet problemleridir.

Problemlerin birincisi ile ilgili olarak, sistemin merkezi olmayan bağımsız bir yapıda olması hem güvenlik hem de bağımlılıklar anlamında kolaylık sağlamaktadır. Başka merkezi

sistemlerle bağımlılığın olmaması başka sistemlerdeki güvenlik açıkları ve başka sistemlerin yönetimi ile ilgili hususları ortadan kaldırmaktadır. Bu sebepten merkezi olmayan blokzincir yapısının kullanılması önemli bir problemi ortadan kaldırmaktadır.

İkinci problem ile ilgili olarak, mobilitesi yüksek sistemlerde haberleşmenin hızlı gerçekleşmesi çok önemlidir. Bu sebepten blokzincirler içerisinde genel blokzincir kullanılmamaktadır. Özel blokzincirde ise aynı anda gelecek birden çok isteğin karşılanmasının zorluğu ve veri kaybına yol açma ihtimalinden dolayı konsorsiyum blokzincir kullanılmaktadır.

Üçüncü problem için ise veri bütünlüğü konusunun sağlanmasıdır. Bunu sağlamak için de güncelleme işlemi bulunmayan ve tüm işlemlerin kayıt altında tutulduğu blokzincir teknolojisi kullanılmaktadır.

Dördüncü ve son problemi ele aldığımızda mahremiyeti sağlamak için sistemimiz açık ve kapalı anahtar oluşturmaktadır. Bu anahtarların yönetimini de yine konsorsiyum havuzu ve düğümleri birlikte yönetmektedir. Bu sayede merkezi olmayan bir yapı ile mahremiyet konusu da ele alınmaktadır.

1.2. NEDEN BLOK ZİNCİR

Blok Zincir veritabanı, hükümet veya finans kurumu gibi merkezi bir otorite yerine, bir bilgisayar ağı tarafından tutulan merkezi olmayan bir dijital işlem defteridir. Blok zincirleri ve daha geniş çapta dağıtılmış defterler esasen merkezi olmayan veritabanları olsa da, blok zincir düğümleri genellikle büyük veri hacimlerini depolamak için temel bir veritabanına ihtiyaç duyar.

Zincirdeki her blok, birden fazla veritabanı işleminin kaydını içerir ve her blok, kendisinden önce gelen blokla bağlantılıdır. Bu sürekli, kesintisiz bir bilgi zinciri oluşturur. Bu blok zincir özellikleri, bir işlemin kaydedildikten sonra değiştirilmesini veya silinmesini çok zorlaştırır; çünkü herhangi bir değişikliğin, veritabanını koruyan blockchain bilgisayar ağı tarafından onaylanması gerekir.

Blok Zincir dağıtılmış veritabanları merkezi olmayan ve şifrelenmiş olduğundan, finans, sağlık ve tedarik zinciri yönetimi gibi sektörlerde genellikle güvenli ve şeffaf kayıt tutmak için kullanılırlar. Bitcoin gibi kripto para birimleri de işlem sistemlerinin temeli olarak blok zincir teknolojisini kullanılmaktadır.

Blok Zincir veritabanı nedir ve geleneksel veri depolama modellerinden farkları aşağıdaki maddelerle gösterilmektedir:

- Merkezi Olmama: Blok Zincir'in geleneksel depolamaya göre temel avantajlarından biri merkeziyetsizliktir. Tipik olarak, geleneksel veritabanları merkezileştirilmiştir; bu, tek bir saldırı noktasını temsil eden hükümet veya şirket gibi tek bir kuruluş tarafından kontrol edildikleri anlamına gelir. Blok Zincir, bilgisayarlardan oluşan bir ağ boyunca korunduğu, saldırı noktalarını ve riski dağıttığı için kurcalamaya veya hacklenmeye karşı daha dayanıklıdır.
- Değişmezlik: Blok Zincir'in geleneksel depolama tasarımına göre önemli avantajlarından bir diğeri de değişmezliktir. Bu aynı zamanda merkezi olmayan ancak hala blok zincir platformları üzerine kurulmamış ve bu nedenle değişmezlik, şeffaflık ve diğer blok zincir özelliklerinden yoksun blok zincir modelleri arasındaki farktır. Veriler bir blok zincir'e eklendiğinde ağdan fikir birliğine varılmadan silinemez veya değiştirilemez.
- Güvenlik: Blok Zincir depolamasındaki ek bir fark, blok zincir tabanlı veritabanlarının kullandığı kriptografidir. Geleneksel veritabanları erişim kontrollerine ve diğer güvenlik önlemlerine güvenerek verileri daha az güvenli hale getirir.
- Şeffaflık: Blok Zincirleri tasarım gereği şeffaftır, böylece tüm kullanıcılar blok zincirine eklenen tüm işlemleri görebilir. Bunun aksine, geleneksel depolama, herhangi bir belirli veriye veya işleme erişimi sınırlandıracak şekilde tasarlanabilir.
- Uzlaşma Mekanizması: Blok zincirleri, işlemleri doğrulamak ve bunları veritabanına eklemek için bir fikir birliği mekanizmasına dayanır. Bu, ağdaki tüm kullanıcıların, bir işlemin blok zincir'e eklenmeden önce geçerliliğini kabul etmesini gerektirir. Geleneksel depolama modelleri bu düzeyde bir fikir birliğine ihtiyaç duymaz.

1.3. NEDEN KONSORSİYUM BLOK ZİNCİR

Konsorsiyum Blok Zincir'in diğer blok zincir türlerine göre faydaları maddeler halinde aşağıdaki gibi listelenmektedir:

- Daha Fazla Verimlilik: Ağdaki düğüm sayısı güvenilir bir katılımcı grubuyla sınırlı olduğundan, konsorsiyum blok zincirleri halka açık blok zincirlerden daha verimli olabilir. Sonuç olarak, işlem doğrulama daha az hesaplama kapasitesi gerektirir, bu da daha hızlı işlem süreleri ve daha ucuz ücretler sağlar.
- Gelişmiş Güvenlik: Tanınmış ve güvenilir üyelerden oluşan küçük bir grup, konsorsiyum blok zincirlerini kontrol ettiğinden, bunlar halka açık blok zincirlerden daha güvenlidir. Bu nedenle kötü aktörlerin ağı manipüle etmesi veya dolandırıcılık işlemleri gerçekleştirmesi daha zordur.
- Paylaşılan Maliyetler: Konsorsiyum blok zinciri tutmak, özel bir blok zincir ağı oluşturmak ve sürdürmekten daha ucuz olabilir çünkü maliyetler üyeler arasında paylaştırılır.
- Daha İyi Veri Gizliliği: Daha küçük bir saygın üye grubu ağa erişebildiği için konsorsiyum blok zincirleri, halka açık blok zincirlerden daha fazla veri gizliliği sunar. Bu nedenle veri gizliliğinin çok önemli olduğu ticari kullanım durumları için daha uygundur.
- Daha Fazla Kontrol: İşbirliğine dayalı bir blockchainde her katılımcı ağ yönetimini ve işlem doğrulamayı etkileyebilir. Sonuç olarak, herkesin ağın başarısından çıkarı olması nedeniyle daha iyi bir yönetim ve karar alma süreci söz konusu olabilir.
- Ölçeklenebilirlik: Konsorsiyum blok zincirleri, katılımcı sayısı sınırlı olduğundan halka açık blok zincirlerden daha verimli bir şekilde ölçeklenebilir. Bu, ağın performansını etkilemeden işlem işleme kapasitesinin artırılabileceği anlamına gelmektedir.
- Özelleştirilebilir Yönetişim: Konsorsiyum blok zincirinde katılımcılar yönetim modelini kendi özel ihtiyaçlarına göre özelleştirebilir. Bu, karar vermede daha fazla esneklik sağlar ve ağın katılımcıların çıkarlarıyla uyumlu olmasını sağlamaya yardımcı olur.
- Birlikte Çalışabilirlik: Konsorsiyum blok zincirleri, diğer blok zincir ağları veya geleneksel sistemlerle birlikte çalışacak şekilde tasarlanabilir. Bu, iş süreçlerini kolaylaştırmaya ve verimliliği artırmaya yardımcı olabilir.
- Azaltılmış Düzenleme Yükü: Konsorsiyum blok zincirleri güvenilir bir katılımcı grubuyla sınırlı olduğundan, mevzuat uyumluluğunu yönetmek daha kolay olabilir. Bu, kuruluşların üzerindeki düzenleme yükünün azaltılmasına ve uyumluluk maliyetinin düşürülmesine yardımcı olabilir.

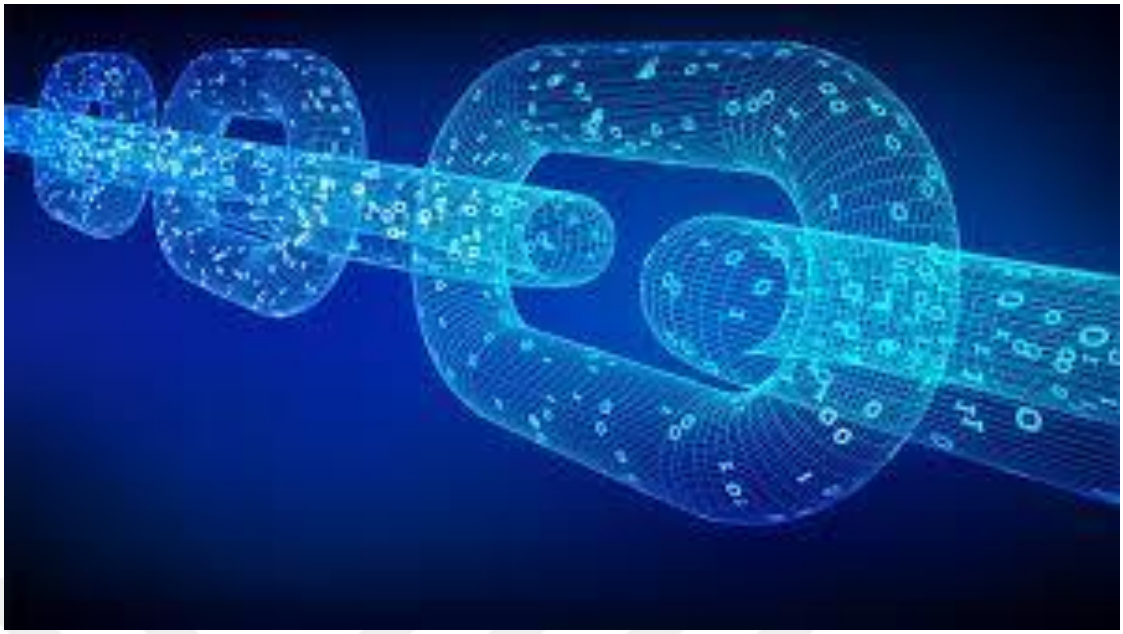
- İşbirlikçi İnovasyon: Konsorsiyum blok zincirleri, katılımcılar arasında işbirlikçi inovasyonu teşvik etmek için kullanılabilir. Katılımcılar, kaynakları ve uzmanlığı paylaşarak tüm ağa fayda sağlayacak yeni çözümler ve uygulamalar geliştirebilirler.

2. KAVRAMSAL ÇERÇEVE

Kavramsal çerçeve olarak iki ana konu bulunmaktadır. Bunlar VANET ve Blok Zincir'dir.

2.1. BLOK ZİNCİR

Birçok araştırmacı blok zincir üzerinde çalışmaktadır. Her araştırmacının bu konuda birçok yorumu vardır. Reyna, çalışmalarında blok zincir teknolojisini kullanarak yapılan işlemlerin güvenilirliğinin bağlı ağdaki paydaşlar tarafından doğrulandığı dağıtık, izlenebilir, değişmez ve güvenli bir veri yapısı sunmaktadır [28]. Glaser, kullanıcıları arasında belirlenen ağda paylaşılan ve kritik bilgilerin kayıtlarının merkezi bir otoriteye ihtiyaç duymadan tutulduğu, yani herkes tarafından bağımsız olarak kullanılan ve takma isimler kullanılarak tutulan bir veri tabanı olarak tanımladığı blok zincirini kullanmaktadır [29]. Zheng ise bu teknolojiyi, tüm işlemlerin blok listelerinde tutulduğu ve yeni bloklar eklendikçe büyüdüğü bir büyük veri defteri olarak tanımlanmakta ve blok zincirini bu şekilde kullanmaktadır [30]. Nakamoto'ya göre blok zinciri teknolojisi, her işlem bilgisinin ağdaki diğer katılımcılar tarafından saklandığı ve ağdaki diğer katılımcılarla paylaşıldığı dağıtılmış bir veri yapısıdır [31]. Beck'e göre blok zincir teknolojisi, bulunduğu ağda çok sayıda düğümle yani katılımcılarla etkileşime girerek tutarlı işlemler sağlayan ve kendi ürettiği bir veri setidir [32]. Tama, amacı veri bütünlüğünü sağlamak olan dağıtık bir yazılım sisteminin parçası olarak tanımladığı blok zincirini bu şekilde kullanmaktadır [33].



Şekil 2.1: Blok Zincir.

Blok zincirinde bulunan özel özellikler, araştırmacıların onu çeşitli alanlarda kullanmakla ilgilenmelerini sağlamaktadır. Örneğin, blok zincir endüstri 4.0 [4,34], Nesnelerin İnterneti (IoT) [5], Akıllı şebeke [6], akıllı havaalanları [7], akıllı tıp [8] vb. alanlarda kullanılmaktadır.

Benzer şekilde, bulut depolama ve diğer mobil hizmetlerle işbirliği yapılarak, blok zincir tabanlı sistemlerin verimliliği, kullanılabilirliği ve güvenilirliği arttırılmaktadır. ITS'de (Intelligent Transportation System) blok zincir kullanımı, kaynak kimlik doğrulaması [9], güven ve itibar yönetimi [10], olay ve mesaj alışverişi yönetimi [11], akıllı ödeme [12], trafik araştırması [13] vb. sağlamak için benzer avantajlar elde etmek için kullanımı artmaktadır.

IoV'lerin gerçekliğini sağlamak için daha önce birkaç kimlik doğrulama yöntemi önerilmektedir. Bazı araştırmacılar, bazılarının kimlik doğrulama için blok zincir kullandığı IoV'lerin kimliğini doğrulamak için Sertifika Yetkilisi'ni (Merkezi Otorite)(CA) önermektedir. Örneğin, kimlik doğrulama ve devir işleminin verimliliğini artırmak için Lai ve ark. blok zincirinin araçlar, yönlendiriciler ve kontrol veritabanları arasında bilgi paylaşmak için kullanıldığı bir sistem önerilmektedir [14]. [16] 'da Ali ve ark. Yetkili ve yetkisiz araç bilgilerini ayrı ayrı depolamak için birkaç blok zinciri kullanmaktadır. Ancak, sertifika tabanlı sistemin ek yükünü ortadan kaldırmak için Ali ve ark. sertifikasız bir kimlik doğrulama protokolü önermektedir.

Benzer şekilde, [17,18]'de, iki farklı blok zinciri, araçlar arasında iletilen mesajları saklamak için başka bir blok zincirinin bulunduğu, sertifikalı ve iptal edilmiş araçların bilgilerini depolamaktadır. Yalnızca araçlar değil, altyapının güven bilgileri de [12] 'da akıllı bir ödeme sistemi geliştirmek için bir blok zincirinde saklanmaktadır. Herhangi bir işlemden önce, hem nakit sayacı hem de sürücü birbirlerinin gerçekliğini kontrol eder ve işlem bilgileri de blok zincirinde saklanmaktadır.

[15]'de Javaid ve ark. kimlik doğrulama için CA'yı ve kimlik doğrulama bilgilerini depolamak için blok zincirini kullanır, ancak çalışmada işaret ve doğrulama ek yükünden bahsedilmemektedir. [19]'da, Zhang ve ark. kimlik doğrulama bilgilerinin konum ve yön bilgileriyle depolandığı blok zinciri tabanlı bir depolama sistemi önermektedir. Bununla birlikte, sertifika oluşturma, imzalama ve doğrulama, yüksek ek yük oluşturmaktadır.

Kimlik doğrulama bilgilerinin depolanması ve araçların blok zincirinin gizliliğinin korunması [20]'de kullanılmaktadır. Güvenlik hizmetlerini artırmak için, yöntem yüksek hesaplama yükü oluşturmaktadır. Benzer şekilde, [19-25,35] gibi diğer bazı protokoller, kimlik doğrulama işlemlerini tamamlamak için çok zaman gerektirmektedir. Ek olarak, araçların kimlik doğrulama bilgilerinin Li ve diğerleri tarafından önerilen bir yöntemle depolanması ve Salem vd. çok fazla depolama alanı gerektirmektedir [27,36].

RSU'ya bağlı olarak yukarıda bahsedilen protokollerin tümü, pahalı altyapı destekleri gerektirmektedir [37]. Bununla birlikte, tipik sertifika tabanlı protokoller, hafif şifrelemeli blok zinciri tabanlı sistemin daha az ek yük ürettiği ve ek olarak tipik blok zincirinin ekstra olanaklarını sağladığı durumlarda daha yüksek ek yük oluşturmaktadır [9].

İletişimin güvenilirliğini artırmak ve VSN(Vehicle Social Network) alanını geliştirmek için işbirliğinin etkinliği zaten kanıtlanmaktadır [38]. VANET'lerin performansını iyileştirmek için araştırmacılar tarafından çeşitli işbirliği protokolleri sunulmaktadır. [39]'da, küme tabanlı VANET için yalnızca Acil Durum Mesaj İletimi (EMT) için uygun olan bir ortak yöntem önerilmektedir. Ancak işbirliği kanalın serbest olması halinde kurulabilmektedir. Woo ve ark. sadece EMT(Emergency Message Transportation) için geçerli bir işbirliği protokolü önerdi ve hareketliliğin etkisi dikkate alınmamaktadır [40]. Taghizadeh ve diğerleri tarafından önerilen yöntem aynı zamanda yalnızca EM içindir, ancak 100 ms'lik SDR'yi (Standard Delay Requirements) karşılayamamaktadır [13]. Benzer şekilde, Zhang ve diğerleri tarafından

eşzamanlı iletim tabanlı MAC protokolü ayrıca SDR'yi karşılamaz ve sadece GMT'ler (General Message Transportation) için uygundur [41].

[42]'de, Zhou ve ark. Gönderme İsteği / Göndermeyi Temizle (RTS / CTS) mekanizmasını kullanarak ortak bir şema sunmakta, ancak kanalda ek yük yarattı ve çarpışma olasılığını artırmaktadır. Ayrıca, RTS/CTS tabanlı yöntem EMT için uygun değildir.

[43]'de ortak bir indirme protokolü sunulmakta ve [44]'da kaynakların kullanılabilirliğini artırmak için bir aktarmalı yayın sunulmakta, ancak hiçbiri iletim protokollerinin gecikmesini açıklamamaktadır.

Bazı araştırmacılar, blok zincirinin ayrıntılı yönlerini dikkate almadan yalnızca veri bütünlüğüne odaklanmaktadır. Örneğin Halpin, blok zincirini yalnızca kriptografik olarak doğrulanabilir bir veri listesi olarak tanımlamaktadır [45]. Teknik olarak bu konuya baktığımızda blok zinciri tanımlarsak aslında dağıtık bir veri tabanı, bağımsız, merkezi bir yapıya ihtiyaç duymayan bir mekanizma, kriptografik şifreleme ve hash mekanizması için kullanılan algoritmaların bir kombinasyonu olarak tanımlanabilmektedir. Blok zinciri teknolojisinde kullanılan işlem verileri, şifreleme algoritmaları kullanılarak birbirine bağlanır ve kullanım potansiyeli olan sonsuz bir dizi veri bloğunda tutulmaktadır. Bu blokların oluşumu, işlemlerin doğruluğu ve geçerliliği için merkezi olmayan zaman damgalı algoritmalar aracılığıyla katılımcı düğümler tarafından oylanarak sağlanmaktadır [46]. Zhao'nun çalışması, blok zincirinin en önemli özelliğinin insanlar yerine ağ tabanlı hesaplamalar aracılığıyla güvenilir ve şeffaf işlemler sağlaması olduğunu göstermektedir [47]. Bu özelliği ile blok zinciri "etkileşimler için bir işletim sistemi" olarak ifade edilebilmektedir [48]. Lewis'e göre blok zinciri teknolojisi ile geleneksel veri tabanları arasındaki temel fark, blok zinciri teknolojisinin yeni veri ekleme, eklenen bilgileri doğrulama ve paylaşım gibi işlemler için P2P ağı üzerinde çalışarak kural tabanlı çözümler sunabilen oldukça gelişmiş bir tür olmasıdır [49]. Blok zincirinin avantaj ve dezavantajlarını şu şekilde sıralanabilmektedir [50].

- Blok zincirinin avantajları: Tüm veriler blok zincirinde yer alan tüm paydaşlarda bir kopya olarak saklanmaktadır. Bu sayede hem hatalı verinin hem de veri kaybının önüne geçilmiş olur. Bu sayede merkezi bir otorite olmadan da çalışabilen bir yapı haline gelir. Ayrıca dijital imzalama veya doğrulama süreçleri sayesinde aracı olmadan da güven sağlanabilmektedir. Çünkü tüm paydaşlar hem kendi işlem durumlarını hem de tüm

işlemlerin detaylarını görebilmektedir. Ayrıca blok zincirinde yer alan bilgiler değiştirilemez veya silinemez.

- Blok zincirinin dezavantajları: Blok zincirinin sonu olmadığı için yüksek bir işlemci ve depolama maliyeti gerektirir. Bu yüzden çok fazla enerji tüketir. Ayrıca kullanılan tüm verilerin her düğümde ayrı ayrı saklanması ve bu düğümlerdeki verilerin tutarlılığının her işlemden sonra sağlanması nedeniyle geleneksel veri tabanlarına göre performans açısından yetersiz kalmaktadır. Güvenlik açısından, ağdaki her bir düğümün tüm verilerin bir kopyasını saklama ve içeriğine erişme yeteneği nedeniyle kullanıcıların gizliliği tehlikeye girebilir.

Mevcut blok zinciri sistemleri üç kategoride sınıflandırılır: Genel blok zinciri, Özel blok zinciri ve Konsorsiyum blok zinciri [51-52].

2.1.1. Genel Blok Zinciri

Genel Blok Zinciri, çeşitli kurumlara bağlı veya bağımsız kişilerin katılmasına, kayıt eklemesine izin veren açık bir platform sağlamaktadır. Bu blok zincirinin herhangi bir kısıtlaması yoktur ve bu nedenle izinsiz blok zinciri olarak da adlandırılmaktadır. Genel blok zincirleri tamamen açık ve şeffaftır ve herhangi bir özel doğrulayıcı düğüm içermemektedir [51].

Şekil 2.2: Genel Blok Zincir.

Herkesin tüm zincir verilerini indirebilmesi ve blok zincirinde madenciliğe başlayabilmesi, zincirin birçok aktif kopyasının olmasını sağlamaktadır. Bu, blok zincirinin güvenliğini ve tutarlılığını artırmaktadır. Bu sayede herhangi bir kontrol mekanizması olmayan dağıtılmış yapılarda, mevcut ağdaki veri boyutunun büyümesi nedeniyle zincirdeki bir değişiklik sırasında konsensüs protokollerine çok fazla iş düşmektedir [52].

2.1.2. Özel Blok Zinciri

Bir kişi veya grup tarafından yönetilen, bir veya birden fazla kuruluşta bireyler arasında veri alışverişini ve paylaşımını sağlayan özel blok zincir yapılarına Özel blok zincirleri denir. Özel bir izne sahip olmayan kişiler zincire katılamadığı için izinli blok zinciri olarak da adlandırılabilmektedir. Bir düğümün ağa katılımı ve erişimi, ağı yöneten grubun belirlediği kurallara göre yapılmaktadır. Bu, blok zincirinin merkezi olmayan ve şeffaf doğasının uygunluğunu azaltmaktadır [51-52].

2.1.3. Konsorsiyum Blok Zinciri

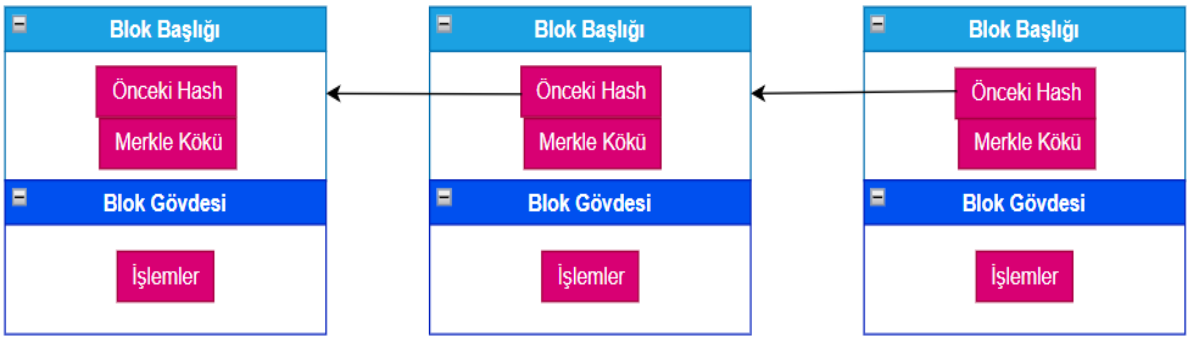
Konsorsiyum blok zinciri, blok zincirindeki her bir bloğun doğrulanması ve fikir birliği gibi süreçlerde tek bir yapıdan ziyade, önceden belirlenmiş ve seçilmiş bir düğüm grubunun karar verici olduğu, kısmen özel ve izinli bir blok zinciri yapısı olarak tanımlanabilmektedir. Bu belirlenmiş düğümler, hangi katılımcıların blok zinciri ağına katılacağına ve hangi katılımcıların veri madenciliği yapabileceğine karar vermektedir. Blok zincirindeki her blok doğrulaması için, ilgili bloğun yalnızca yetkili düğümler tarafından imzalanması yeterli olduğunda çoklu imza şeması kullanılmaktadır. Bir konsorsiyum, ağın genel mi yoksa sınırlı mı olduğuna ve ağdaki herkesin veri okuma ve yazma işlemlerine sahip olup olmadığına karar vermektedir [51-52].

2.1.4. Blok Zinciri Yapısı

Şekil 2.1, blok zinciri yapısının bir örneğini göstermektedir. Bir bloğun yalnızca bir ana bloğu vardır ve her bloğun başlığı önceki bloğun özet bilgilerini içermektedir. Blok zinciri teknolojisinde, zincirdeki ilk blok, bağlı olduğu bir ana bloğa sahip olmayan genesis bloğu olarak tanımlanmaktadır.

Blok zinciri teknolojisindeki her blok bir gövde ve bir başlıktan oluşmaktadır. Blok başlığında yer alan bilgiler: Blok sürümü, Merkle ağacı kök karması, Zaman Damgası, geçerli bir blok karma değeri için eşik bilgisi, Nonce (genellikle 0 ile başlayan her hesaplama için artan 4

baytlık bir alan) ve Önceki blokta hash alanı Bir önceki bloğa karşılık gelen 256 bitlik bir özet değeri zincirde tutulmaktadır [53].



Şekil 2.3: Blok Zinciri Yapısı [28].

Blok zinciri teknolojisindeki her blok gövdesi, kaydedilen işlem bilgilerini ve işlem sayısını tutan bir sayaçtan oluşmaktadır. Blok zincirindeki her bloğun barındırabileceği maksimum işlem sayısı, ilgili bloğun kapladığı alana ve her işlemin boyutuna bağlı olarak değişebilmektedir. Blok zincirindeki her işlem doğrulaması, asimetrik bir şifreleme mekanizmasıyla birlikte kullanılan bir dijital imza ile onaylanmaktadır.

Dijital imza, blok zinciri teknolojisinde tutulan verilerin bütünlüğünü ve güvenliğini sağlamanın en temel yöntemlerinden biridir. Dijital imzalar asimetrik şifreleme kullanmaktadır. Ayrıca, dijital imzalar, şifrelenmiş bilgilerin ortak anahtarı kullanılarak paylaşılabilmektedir. Blok zinciri teknolojisini kullanan yapılarda her katılımcının bir ortak anahtarı ve bir özel anahtarı vardır. Katılımcılar, işlemlerini imzalamak için özel anahtarı kullanmaktadır. Ayrıca özel anahtarlar gizli tutulmaktadır. Uygulanan dijital imzalarla yapılan işlemler, tüm blok zinciri ağında yayınlanmaktadır. Dijital imza süreci iki farklı aşama olarak belirtilebilmektedir. Bu aşamalar imzalama ve doğrulama olarak sıralanmaktadır. Örneğin, bir kullanıcının başka bir kullanıcıya dijital olarak imzalanmış bir mesaj göndermesi gerektiğinde, önce imzalaması gerekmektedir. Bu imzalama aşamasında mesajı gönderecek olan kullanıcı kendi özel anahtarı ile verileri şifreler ve şifrelenmiş mesajı ve orijinal veriyi mesajın gönderileceği kullanıcıya göndermektedir. Bundan sonra ikinci aşama olan doğrulama aşaması gelmektedir. Bu

doğrulama aşamasında mesajı alan kullanıcı, mesajı gönderen kullanıcının açık anahtarı ile alınan mesajın değiştirilip değiştirilmediğini kolaylıkla kontrol eder ve mesajı alır.

Blok zincirinde veri içeren her işlemin zincire eklenmesi sonucunda zincirin boyutu giderek artmaktadır. İşlemlerin boyutu belirli bir büyüklüğe ulaştıktan sonra yeni bir blok oluşturulur ve önceki blokla ilişkilendirilerek zincire eklenmektedir.

2.1.5. Blokzincir Türlerinin Kıyaslanması

Şekil 2.2'de görüldüğü üzere genel blok zincir performansın düşük olması ile hız gerektiren yapılarda pek kullanılabilir olmadığı görülmektedir. Konsorsiyum ve Özel blok zincir ise daha performanslı yapılar olduğu görülmektedir.

	Genel Blok Zincir	Konsorsiyum Blok Zincir	Özel Blok Zincir
Merkeziyetsizlik	Evet	Evet/Kısmi	Kısmi
Okuma Yetkisi	Tüm Düğümler	Seçilmiş Düğümler	Bir Düğüm
Karar Verme Mekanizması	Tüm Düğümler	Seçilmiş Düğümler	Bir Düğüm
Üretkenlik ve Performans	Düşük	Yüksek	Yüksek
Uzlaşma Süreci	Otoritesiz	Otoriteli	Otoriteli

Şekil 2.4: Blok Zincir Çeşitlerinin Kıyaslanması.

Sistemimizde Konsorsiyum blok zincir kullanılmaktadır. Blok zincirlerde konsensus mekanizmaları bulunmaktadır. Blok zinciri merkezi olmadığı için, blok zincirindeki işlemleri doğrulamak için büyük ölçüde bir fikir birliği mekanizmasına dayanmaktadır. Ayrıca, fikir

birliğinin hızı, kullanılan fikir birliği yönteminin türüne bağlıdır. Bazı fikir birliği yöntemleri diğerlerinden daha hızlıdır. Bunlar:

- İş Kanıtı (Proof of Work - PoW)
- Varlık Kanıtı (Proof of Stake - PoS)
- Otorite Kanıtı (Proof of Authority - PoA)

2.1.6. İş Kanıtı

İş Kanıtı (Proof of Work - PoW) isminde de anlaşılacağı üzere blok eklemek için emek gerektiren bir uzlaşma yöntemidir. PoW, Bitcoin kripto parasının kullandığı bir yöntemdir. Hesaplanması kolay olmayan kriptografik bilmecelere dayanmaktadır. Bu bilmeceleri çözmeye çalışan ağdaki düğüme madenci denir. Belirlenen özet değerini elde eden ilk düğüm blok zincirin sonuna blok ekleme hakkına sahip olmaktadır. Eğer aynı anda birden fazla madenci aynı özet değerini aynı anda elde ederse ve ağa gönderirse bir çatallanma gerçekleşmektedir. Bu durumda çatalların birinde yeni bir blok üretilene kadar iki çatal da bulunmaya devam etmektedir. Hangisine yeni bir blok eklenirse uzun çatalda madenciler çalışmalarına devam ederler. Matematiksel çözümlerin zorluğundan dolayı çok fazla bilgisayar gücüne gereksinimi vardır ve çok zaman harcanmaktadır.

2.1.7. Varlık Kanıtı

Varlık Kanıtı (Proof of Stake - PoS) Çok fazla enerji harcayan PoW algoritmasına alternatif olarak PoS uzlaşması ortaya konulmaktadır. Bu uzlaşma yönteminde ağdaki düğümler arasında fazla varlık hissesi olanlar blok ekleme hakkı elde ederler. Bu yüzden kripto paralarının miktarını ispatlaması gerekmektedir. PoW'daki gibi bir kriptografik bilmece çözme gerektirmediği için işlem gücü fazla değildir. Ancak en fazla hissesi olan düğüm hep baskın olabileceğinden dolayı bir sonraki bloğu yaymak için varlıkların oluşturulma zamanı gibi bilgilere bakılarak çözümler sunulmaktadır.

2.1.8. Otorite Kanıtı

Otorite Kanıtı (Proof of Authority - PoA) Diğer uzlaşma yöntemlerine göre birkaç önemli avantajı bulunmaktadır. PoW ve PoS yöntemlerine göre belli sayıda blok doğrulayıcısı olduğu için daha ölçeklenebilmektedir. Dijital kimliklerle bloklar onaylanır. Dolayısıyla kripto para miktarı yerine kendi itibarlarını kullanmaktadır. Yeni blokların üretildiği zaman aralığı tahmin edilebilmektedir. PoW ve PoS mutabakatı için bu süre değişir. Yüksek işlem oranı vardır.

Bloklar, yetkili ağ düğümleri tarafından belirlenen zaman aralığında bir sırada oluşturulmaktadır. Bu da, işlemlerin onaylanma hızını artırır. PoA'nın kullanıldığı bir örnek olarak Microsoft Azure verilebilir. Özel ağlara alternatif bir çözüm olarak sunularak madencilik yapılmasına ihtiyaç olmaz.

Otorite Kanıtının Avantajları şu şekilde sıralanabilir:

- %51 saldırısı daha zor
- Yeni blokların oluşturulduğu zaman aralığı tahmin edilebilir. PoW ve PoS konsensüsleri için bu süre değişmektedir.
- Yüksek işlem oranı.
- Proof of Work gibi hesaplama gücü gerektiren algoritmalardan çok daha sürdürülebilir.
- Yüksek performanslı donanım gerekli değildir. PoW konsensüsü ile karşılaştırıldığında, PoA konsensüsü, düğümlerin karmaşık matematiksel görevleri çözmek için hesaplama kaynakları harcamasını gerektirmez.
- Bloklar, yetkili ağ düğümleri tarafından atanan zaman aralığında bir sırayla oluşturulur. Bu, işlemlerin doğrulanma hızını artırır.

2.2. BLOKZİNCİRDE GÜVENLİK ATAKLARI

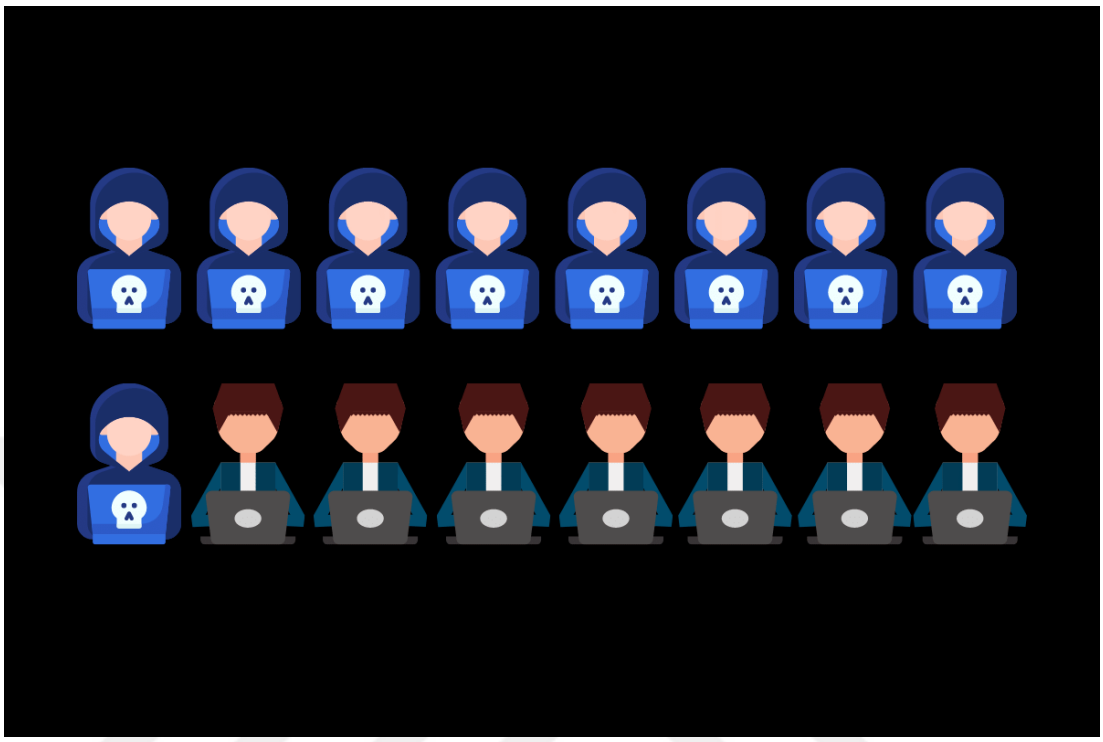
Blok Zincir teknolojisi değiştirilemez bir defter(ledger) kullanırken, teknolojinin temel doğasını bile tehdit edebilecek bazı blok zincir güvenlik sorunları mevcuttur. Bu güvenlik sorunları bu başlık altında ele alınmaktadır.

2.2.1. %51 Saldırısı

Yukarıda tartıştığımız gibi madenciler, blok zincir üzerindeki işlemlerin doğrulanmasında önemli bir rol oynamakta ve böylece blok zincirinin daha da büyümesine yardımcı olmaktadır. Blok Zincir teknolojisi, popüler desteğe dayalı kararlar almaktadır. Örneğin, bazen çakışan işlemlerle aynı anda iki blok çıkarılmaktadır. Bu durumda ağda çoğunluk onayını alan blok zincirde kalır, diğeri ise zincire eklenmez.

Şimdi, eğer bir grup kötü niyetli bilgisayar korsanı madencilik gücünün %51 veya daha fazlasının kontrolünü ele geçirmeyi başarırsa, sonuçlar felaket olabilmektedir. Bilgisayar korsanları daha sonra işlemleri iptal etmek ve hileli işlemler gerçekleştirmek için çoğunluk

konumlarını kullanabilmektedir. Hatta bazı blokları yeniden yazabilirler, ancak tüm blok zincirini yeniden yazmak (teorik olarak mümkün olsa da) neredeyse imkansızdır.



Şekil 2.5: %51 Saldırısı.

%51 saldırısı gibi blok zincir güvenlik sorunlarının zincirin ilk aşamalarında meydana gelme olasılığı daha yüksektir. Ağda çok az madencinin bulunduğu bir dönemde madencilik gücünün %51'ini ele geçirmek mümkün olabilmektedir. Sybil Saldırıları %51 için en önemli örneklerden biridir. Adını ünlü bir kitap karakterinden alan bu saldırı türünde, saldırgan ağ üzerinde birden fazla sahte düğüm oluşturmaktadır. Saldırgan bu düğümleri kullanarak çoğunluk konsensüsü elde edebilmekte ve zincirdeki işlemleri engelleyebilmektedir. Yani büyük ölçekli bir Sybil saldırısı %51 saldırısından başka bir şey değildir.

Sybil saldırıları gibi blok zincir güvenlik sorunları için birçok blok zincir, iş kanıtı ve hisse kanıtı algoritmalarını kullanmaktadır. Bu algoritmalar bu tür saldırıları tamamen engellemez, yalnızca saldırganın bunları gerçekleştirmesini olanaksız hale getirmektedir.

2.2.2. Çifte Harcama Saldırıları

Fiziksel paranın öne çıkan özelliklerinden biri de aynı faturayı iki farklı yerde kullanarak ödeme yapılamamasıdır. Tam tersine, dijital varlıklar kolayca kopyalanabilmektedir, sonuçta hepsi sadece 1'ler ve 0'lardan ibarettir. Örneğin bir kripto para veya varlık aynı anda iki farklı platform veya cüzdana gönderilebilmektedir. Bu tür saldırılara çift harcama saldırısı adı verilmektedir.

Genellikle bu tür saldırıları engellemek için blok zincir içerisinde yerleşik mekanizmalar bulunmaktadır. Örneğin, eğer kripto para ilk blokta bir kişiye gönderilirse, sonraki bloklarda yapılan tekrar gönderme işlemi göz ardı edilmektedir.

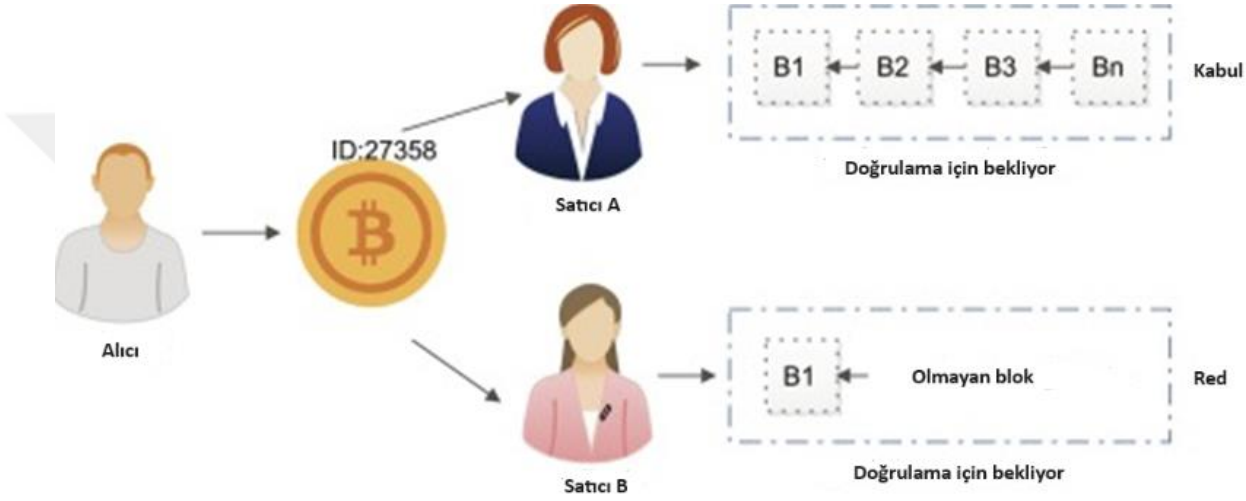
Şekil 2.6: Çifte Harcama Saldırısı.

Ancak her iki işlemin de aynı anda çıkarılan iki farklı bloğa ulaşması durumunda, ağdaki düğümlerden en fazla onay alan blok tutulacak, diğeri bir süre sonra göz ardı edilmektedir. Ancak çifte harcama saldırıları gibi blok zincir güvenlik sorunlarına yönelik bu hafifletme, kendi dezavantajlarını da beraberinde getirmektedir. Sonuç olarak, genellikle kullanıcılar, parayı alma konusunda gerçekten emin olmadan önce (Satoshi Nakamoto'nun teknik incelemesinde önerdiği gibi) en az 6 bloğun daha çıkarılmasını beklemektedir. Üstelik motive olmuş bir saldırgan yukarıda bahsettiğimiz gibi yüzde 51 saldırısını gerçekleştirebilirse daha sonra çift harcama saldırısını rahatlıkla gerçekleştirebilmektedir.

2.2.3. Yönlendirme Saldırıları

Şu ana kadar irdelenen başlıklarla, Blok zincir teknolojisinin çalışması için sağlam bir ağa ihtiyaç duyduğu anlaşılmaktadır. İSS'ler birbirlerine bağlanır ve rota bilgilerini BGP (Sınır Geçidi Protokolü) aracılığıyla paylaşmaktadır. Bu protokol eskidir ve bir saldırganın yararlanabileceği bazı güvenlik açıklarına sahiptir.

Örneğin, bir İSS'yi kontrol eden bir saldırgan, yanlış bir rota yayınlayarak bazı düğümlerin işlemlerini reddedebilmekte, hatta blok zincir ağını ikiye bölebilmektedir.



Şekil 2.7: Yönlendirme Saldırısı.

Yönlendirmeyle ilgili blok zincir güvenlik sorunları, 2014 yılında bir bilgisayar korsanının yönlendirme saldırısını gerçekleştirmesi nedeniyle ciddi sonuçlar doğurabildiği görülmektedir. Bu, bilgisayar korsanının madenciler tarafından çıkarılan blokların ağ üzerinden yayılmasını engellemesine olanak tanımaktadır. Bunun yerine, bilgiyi yapılan işin kendisine ait olduğunu iddia etmek için kullanmakta ve böylece madencilik ücretleriyle ödüllendirilmektedir.

2.2.4. Özel Anahtar Güvenliği Saldırıları

Daha önce de belirtildiği gibi, açık anahtarlı şifreleme, blok zincir teknolojisinin merkezinde yer almaktadır. Bu nedenle, açık anahtar şifrelemesinin yanlış uygulanması veya işlenmesi, bazı ciddi blok zincir güvenlik sorunlarına neden olabilmektedir. Anahtar imzalama blok zincirinizde kötü uygulanmışsa (örneğin, birden fazla imzalama için Merkle ağacı yerine aynı

anahtarın kullanılması), bir saldırganın özel anahtarınızı genel anahtardan almasına olanak tanıyabilmektedir. Özel anahtarınızın kontrolüne sahip olmak, temel olarak sizinle ilişkili tüm verilere bir blok zincirinde sahip olmak anlamına gelmektedir.

Kripto para birimleri söz konusu olduğunda, tüm paralarınıza sahip olurken dikkatli olmak gerekmektedir. Bununla birlikte, blok zinciriniz için gerçekten hatalı kod kullanılmadığı sürece bunun gerçekleşme şansı çok azdır. En büyük sorun, özel anahtarınızın uygunsuz şekilde kullanılmasıdır. Örneğin, virüsün bulaştığı bilgisayarlarda, 2020'de yaklaşık 300 bin dolar değerindeki kripto para birimi, kullanıcının ortak anahtarı Evernote'ta bırakması nedeniyle saldırıya uğramaktadır.

2.2.5. Bencil Madencilik Saldırıları

Bir hesabın bir miktar kripto parayı gecikmeli olarak gönderdiğini ve ayrı işlemlerin birden fazla farklı bloğa dönüştüğünü varsayılmaktadır (insanların birbirlerine para gönderdiği bir dizi başka işlemle birlikte). Bu arada iki farklı hesabın, bu işlemleri doğrulamak için madenciler olarak rekabet ettiği düşünülmektedir.

Sonra bir hesabın ilk işlem için geçerli bloğu bulduğunu ancak bunu ağ üzerinden yaymak yerine sonraki işlemler için ikinci geçerli bloğu bulmak üzere çalışmaya başladığını varsayılmaktadır. Ana blok zinciri, gizli zincirinin bir blok gerisine gelene kadar gizli blok zincirini oluşturmaya devam eder. İşte o zaman stratejik olarak zincirini ağa açıklar. Bazı blok zincir protokolleri tasarlandığından, iki çatalın çakışması durumunda en uzun zincir tutulmaktadır. Dolayısıyla bu işlemi yapan artık daha yüksek bir madencilik ücreti talep edebilmektedir.

Aksine, eğer bu işlemi yapan geçerli bloğu bulur bulmaz yayınlandığında, o ve diğer hesap bir sonraki blok için aynı seviyeden rekabet etmeye başlayabilmektedir. Bu nedenle, bencil madencilik saldırısında saldırgan, kârını en üst düzeye çıkarmak için avantajlı konumunu daha uzun süre elinde tutmak için kullanmaktadır. Ancak bu strateji aynı zamanda risklidir. Eğer diğer hesap ya da başka bir madenci bir sonraki bloğu ilk hesaptan önce bulup yayınlandığında, onun tüm çalışmaları işe yaramaz olmaktadır. Bu, ilk bakışta riskli ve kârsız gibi görünse de Markov zincirlerini kullanan bir analiz, bencil madenciliğin gerçekten işe yaradığını göstermektedir.

2.2.6. Savunmasız Akıllı Kişiler

Akıllı kişiler temel olarak kayıt tutmak için blok zincir kullanan kodla yazılmış anlaşmalardır. Örneğin, gerçek hayatta birine borç verirseniz, borçlanma süresi bitene kadar periyodik olarak faiz alınır ve sonrasında anapara geri alınmaktadır. Artık bu koda çevrilebilmekte ve gerçek para yerine kripto para birimi kullanılabilmektedir. İyi olan şey, banka gibi bir aracıya ihtiyacınızın olmamasıdır. Sözleşme bir kez yürürlüğe girdikten sonra onu değiştirmenin hiçbir yolu yoktur.

Ancak bazen bu kişiler kötü kodlanmaktadır. Bu, saldırganın koddaki potansiyel kusurları bulmasına ve bunlardan yararlanmasına olanak tanımaktadır. Bu durum, bir saldırganın böyle bir kusuru bulup 50 milyon dolar değerindeki kripto para birimini çalmayı başardığı DAO örneğinde görülmektedir.

2.3. V2V

Araç-araç iletişimi, araçların hareket halindeyken kendi aralarında kablosuz ağlar oluşturmasına ve geçici bir ağ üzerinden veri aktarmasına yardımcı olmaktadır. Her araç, trafik ve yol koşulları, aracın konumu ve hızı, rota yönü ve meydana gelmesi durumunda denge ve fren kaybı gibi araç hareketleri hakkında raporlar göndermektedir.

Bilgiler ağa eklenmesi ve diğer araçlar için bir güvenlik uyarısı görevi görmektedir. Trafik radyo istasyonları gibi insanlar için bilgi sağlamaktadır. Bireysel arabalar, çevrelerinden dinamik bir görünüm oluşturmak için ağdaki bilgileri kullanmaktadır. Eksiksiz bir genel bakış, aracın tehlike uyarıları göndermesini ve kazaları önleyen ve trafik sıkışıklığını azaltan eylemleri teşvik etmesini sağlamaktadır [54].

Araç-araç iletişimi, araç-araç (V2V) ve Araç-Altyapı (V2I) olarak adlandırılan iki tür araç iletişim sistemini birleştirmektedir. Sistemler birlikte etkileşimli bir yönlendirme haritası oluşturmaktadır.

Araçların V2V sistemi aracılığıyla konumlarını bildirmesine izin veren GPS alıcıları gibi Nesnelerin İnterneti (IoT) cihazları ve V2I sistemi üzerinden yol koşulları hakkında veri gönderen yol sensörleri sayesinde araçtan araç iletişimine olanak sağlanmaktadır. DSRC (Özel Kısa Menzilli İletişim) iki sistemi birbirine bağlar ve her aracın güvenli navigasyon için gereken tüm bilgileri almasını sağlamaktadır [55].

V2V sistemlerinin ana bileşenleri [56]:

- Özel kısa menzilli iletişim (DSRC): 5.9 GHz bandında 75MHz bant genişliği ile çalışan ve yaklaşık 1000m kısa menzilli kullanım için tasarlanmış kablosuz iletişim kanallarıdır. DSCR, araçtan araç sistemine ve araçtan altyapı sistemine gerçek zamanlı iletişim sağlar. Örneğin; V2V sistemi iletişim kurduğunda, "İtfaiyeci yaklaşıyor" diyebilir. V2I sistemi, "Araba yanıyor, 10 feet, yol engellendi" konusunda uyarı verebilir.
- GPS alıcısı: Araca, yoldaki nesnelerin ve araçların etrafında gezinmesine yardımcı olan gerçek zamanlı konum bilgileri sağlar.
- Ataletsel navigasyon sistemi: Aracın yönlendirme sistemi olarak işlev görür ve her aracın otomobiller ve nesneler arasında güvenli bir şekilde gezinmesine yardımcı olur. Ataletsel navigasyon sistemi, araç üstü sensörlü araçların konumlandırmasını, hızını ve yönünü izler ve tahmin eder.
- Lazer Işıklı Algılama ve Menzil (LiDAR): Aracın çevresine 3B haritalar ve ısı görüntüleri oluşturan bir lazer algılama sistemidir. LiDAR, araçtan nesneye sıçrarken ışığın hızını ölçerek nesneler arasındaki tam mesafeyi hesaplar ve bunun tersi de geçerlidir. Aracın çevresindeki nesnelere yönlenmesine ve altyapı sensörleriyle etkileşime girmesine yardımcı olur.

Araçlar arası haberleşmenin faydaları şu şekilde sıralanabilir[57]:

- Kazaları önler: Araba kazaları her yıl dünya çapında yaklaşık 33.000 kişinin can kaybına neden oluyor ve sayıları her yıl artmaya devam etmektedir. Güvenlik büyük bir endişe haline gelmekte ve farkındalığı artırma ve güvenli sürüş konusunda eğitim alma çabalarına rağmen, araba kazalarının ana nedeni insan hatası olmaya devam etmektedir. Araçlar arası iletişim teknolojisi, insan hatası içeren araç kazalarının% 70 ila% 80'ini azaltmaya yardımcı olabilmektedir.
- Trafik yönetimini iyileştirir ve tıkanıklığı azaltır: Kolluk kuvvetleri, tıkanıklığı azaltmak için araçlardan gerçek zamanlı veri akışı kullanarak trafiği izlemek ve yönetmek için araç-araç iletişimini kullanabilir. V2V iletişimi, yetkililerin trafiği yeniden yönlendirmelerine, araç konumlarını izlemelerine, trafik ışığı programlarını uyarlamalarına ve adres hızı sınırlarına yardımcı olabilir. V2V iletişimi kullanan

sürücüler trafik sıkışıklığını önleyebilir ve diğer araçlarla güvenli bir mesafeyi koruyabilir.

- Kamyon şeritleme ile yakıt verimliliğini arttırır: Araç-araç iletişimi, kamyon filolarının yakın oluşumda sürülmesini sağlar. Öndeki kamyon, paketin lideri olarak hareket eder, ardından tüm kamyonlar takip eder. Takımdaki kamyonlar sürekli formasyonda kalır ve hızlarını ve konumlarını sabit bir iletişim akışına göre ayarlar. Testler, kamyon takım açma işleminin kurşun kamyon için yüzde 5'e kadar ve sonraki kamyonlar için yüzde 10'a kadar tasarruf edebileceğini buldu.
- Güzergahları optimize eder: Araçlar arası iletişim teknolojisine tamamen ticari olarak adapte olunca, yoldaki her araç daha iyi navigasyondan faydalanmaktadır. Tüm araçlar arasındaki açık kanal iletişimi, her aracın rotaları gerçek zamanlı olarak optimize etmesine yardımcı olacak hassas konum, hız ve konumlandırma bilgileri sağlamaktadır.

Birden fazla faktör, aracın araç iletişimine uyumunu engellemektedir. Teknolojinin ticari entegrasyonu, güvenlik sorunlarından protokol standartlarına kadar sistem için ayrılan frekans bandının çok sayıda aracı destekleyememesi endişesine kadar küresel, kamu ve özel sektörde zorluklar ortaya koymaktadır. Bu zorluklardan ötürü bazı sınırlamalar bulunmaktadır. Bu sınırlamalar [58]:

- Güvenlik riskleri: Pürüzsüz bir sürüşün tadını çıkarılabileceği ve sonra aniden başka birinin kontrolü ele aldığı hayal edilebilir mi? Kapılar kilitlenir, tekerlek sizi döndürür, araba motoru hızlanır ve hız sınırını geçer. DSRC'li araçlar siber saldırılara karşı savunmasız olabilir. V2V etkin araçlarda güvenlik ihlalinin sonuçları felaket olabilir ve birden fazla araba terörist saldırılara maruz kalabilir. V2V iletişim sistemleri tam olarak entegre olabilmek için kapsamlı güvenlik önlemleri gerektirmektedir.
- Gizlilik sorunları: V2V ağı, sürücüler hakkında özel bilgiler toplar ve depolar. Şu anda herhangi bir düzenleme olmadığı için, hükümet ve özel şirketler araçları izleme ve sürüş alışkanlıklarını izleme yeteneğine sahiptir. Otomatik Plaka Okuyucularına (ALPR) erişimi olan herkes, araç-araç iletişimi olan araçlar hakkında veri izleyebilir ve toplayabilir. Veriler saldırıya uğramışsa, kimlik hırsızlığına ve diğer güvenlik sorunlarına yol açabilir.

- Sorumluluk endişeleri: V2V teknolojileri hala yeni olduğundan ve açık yasalar ve düzenlemeler olmadığından, V2V araçlarını içeren olaylar sorumluluk endişelerine neden olabilir. V2V iletişim sistemi tarafından verilen talimatlar bir kazaya yol açarsa ne olur? Sistemin talimatlarını yalnızca bir arabanın arkasına çarpıldığında izlenir.
- Potansiyel olarak dikkat dağıtıcı sürücüler: Şu anda, araç-araç iletişim sistemleri çalışmak için insan müdahalesine ihtiyaç duymaktadır. Sürücünün V2V iletişim sistemini çalıştırmak için mesajlaşmaya veya telefonda konuşmaya benzer görevleri gerçekleştirmesi gerekir. İletişim süreci, sürücü için daha az dikkat dağıtıcı olması gerektiği için ya da trafik kazalarının yeni bir nedeni haline gelebileceğinden hala çalışma aşamasındadır.
- Pahalı: V2V iletişim sistemlerinin araçlara kurulumunun maliyeti sistem karmaşıklığına ve araç modeline bağlıdır ve 2.000 ila 20.000 $ arasında değişebilir.

VANET ortamında, kullanılan paketlerin ağ tarafından duyulması nedeniyle merkezi bir kimlik doğrulama sisteminin (sertifika yetkilileri gibi) kullanılması mümkün değildir. Bu ek yük VANET ortamında mümkün değildir [59]. Bu sınırlamanın üstesinden gelmek için alternatif yaklaşımlardan biri, gönderilen mesajın kimlik doğrulamasına güvenmek ve düğümün kimlik doğrulamasını, iletişiminin kimlik doğrulaması yoluyla elde etmek olacaktır.

2.4. AKILLI ARAÇLARDA GÜVENLİK VE BLOKZİNCİR

Akıllı araçlarda kullanılan geleneksel güvenlik ve gizlilik yöntemleri Merkezileştirme, Gizlilik Eksikliği ve Güvenlik Tehditleri zorluklardan dolayı etkisiz olma eğilimindedir [60].

Merkezileştirme, mevcut akıllı araç mimarileri, tüm araçların tanımlandığı, doğrulandığı, yetkilendirildiği ve merkezi bulut sunucuları aracılığıyla bağlandığı merkezi aracılı iletişim modellerine dayanmaktadır. Çok sayıda araç birbirine bağlı olduğundan bu modelin ölçeklenmesi pek olası değildir. Ek olarak, bulut sunucuları bir darboğaz ve tüm ağı kesintiye uğratabilecek tek bir arıza noktası olarak kalmaya devam etmektedir.

Şekil 2.8: Akıllı Araçlarda Güvenlik.

Gizlilik Eksikliği, mevcut güvenli iletişim mimarilerinin çoğu ya kullanıcı gizliliğini dikkate almamaktadır; örneğin, aracın tüm verilerini sahibinin izni olmadan değiş tokuş etmeye başvurmakta ya da talep eden kişiye gürültülü veya özetlenmiş veriler göstermektedir. Ancak birçok akıllı araç uygulamasında, talepte bulunan kişinin kişiselleştirilmiş hizmetler sunabilmesi için kesin araç verilerine ihtiyacı vardır.

Güvenlik Tehditleri: Akıllı araçlarda giderek artan sayıda otonom sürüş fonksiyonu bulunmaktadır. Bir güvenlik ihlalinden kaynaklanan bir arıza (örn. kötü amaçlı yazılım yüklenmesi nedeniyle) ciddi kazalara neden olabilmekte, bu da yolcuların ve yakındaki diğer yol kullanıcılarının güvenliğini tehlikeye atabilmektedir.

Blok Zincir (BZ), birbirine zincirlenmiş blokların giderek büyüyen bir listesini tutan dağıtılmış bir veritabanıdır. BZ ilk olarak Satoshi Nakamoto tarafından Bitcoin'in arkasındaki temel teknoloji olarak önerilmektedir [31]. BZ'nin güvenlik, değişmezlik ve mahremiyet gibi bir dizi göze çarpan özelliğe sahip olduğu ve bu nedenle yukarıda belirtilen zorlukların üstesinden gelmek için yararlı bir teknoloji olabileceği gösterilmektedir. BZ'nin yapısı Şekil 2.1'de gösterilmektedir. BZ, eşler arası bir ağ tarafından dağıtılmış olarak yönetilmektedir. Her düğüm bir ortak anahtar (PK) kullanılarak tanımlanmaktadır. İşlemler olarak bilinen düğümler

arasındaki tüm iletişimler, PK'ler kullanılarak şifrelenir ve tüm ağa yayınlanmaktadır. Her düğüm, işlem oluşturucunun imzasını kendi PK'sine göre doğrulayarak bir işlemi doğrulayabilmektedir. Bu, BZ'nin güvenilir fikir birliğine varabilmesini sağlar; bu, düğümler arasında bir anlaşmanın, sertifika yetkilisi (CA) gibi merkezi bir güven komisyoncusu olmadan gerçekleştirilebileceği anlamına gelmektedir. Bir düğüm, tüm ağa yayınlanan bir blok oluşturmak için, kendi bekleyen işlem havuzundan birden fazla işlemi periyodik olarak toplamaktadır. Blok, tüm bileşen işlemlerinin geçerli olması durumunda, bir düğümde depolanan BZ'nin yerel kopyasına eklenmektedir. Hangi düğümlerin BZ'ye katılabileceğini kontrol etmek için çözülmesi zor, doğrulanması kolay bir bulmacayı çözmeyi içeren Proof of Work (PoW) gibi bir fikir birliği algoritması kullanılmaktadır. Bir blok eklendiğinde, o (veya onu oluşturan işlemler) değiştirilemez, çünkü her bloğun karması zincirdeki sonraki blokta yer alır, bu da değişmezliği sağlar. Bir düğüm, anonimliği ve gizliliği sağlamak için her işlemden sonra PK'sini (yani kimliğini) değiştirebilir.

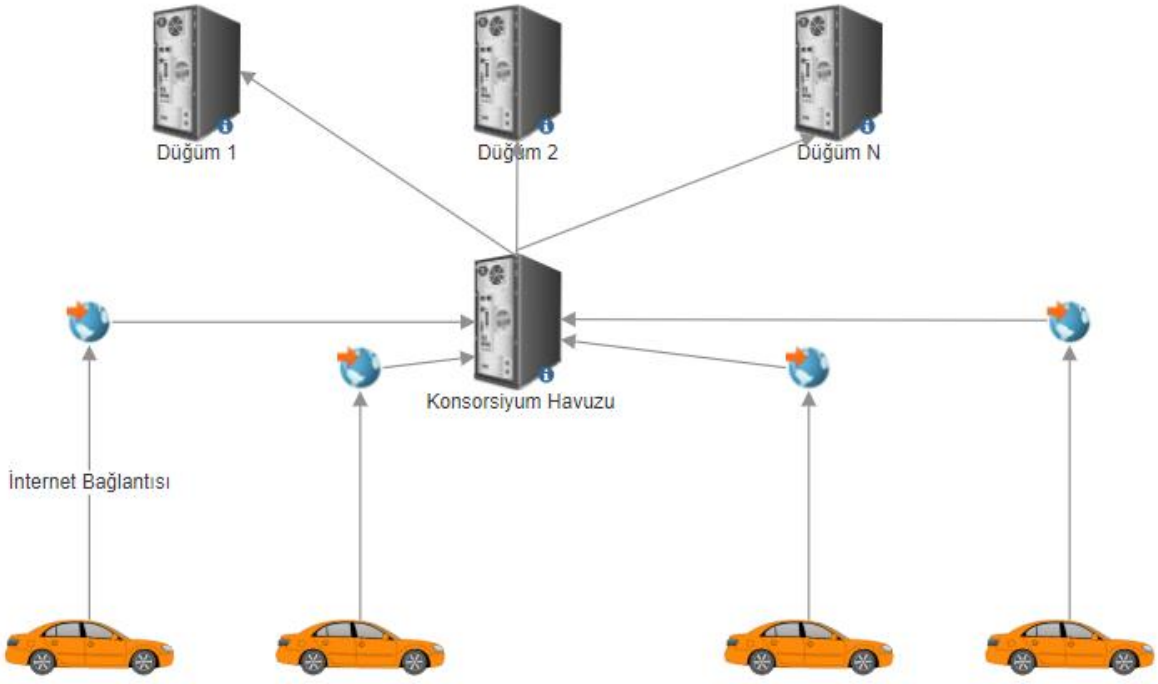
2013 yılında, akıllı sözleşmeleri (yani bir dizi kuralı uygulamaya yönelik bilgisayar programlarını) kolaylaştırmak için Ethereum [61] adı verilen yeni bir açık kaynaklı BZ tabanlı platform önerilmektedir. BlockCharge [62] elektrikli araç şarjına yönelik BZ tabanlı bir platformdur. Temel ödeme yöntemi olarak Bitcoin'i kullanır ve dolayısıyla Bitcoin'in sunduğu yüksek düzeyde gizliliği miras alır. [63]'deki yazarlar, Ethereum BZ'nin araç sahipleri ve hizmet sağlayıcılar arasında dağıtılmış olarak güvenli ve özel akıllı sözleşmeler oluşturmak için kullanılabileceğini savunmaktadır. Ancak bunu destekleyecek bir sistem henüz tasarlanmamıştır. [5]'de, Hafif Ölçeklenebilir Blok Zinciri (LSB) adı verilen IoT için optimize edilmiş bir BZ örneklemesi önermektedir.

3. YÖNTEM

Burada Sistem Yapısı, Sisteme Dahil Olma Süreci, Mesajlaşma Süreci ve Kuyruk Modelinden bahsedilmektedir.

3.1. SİSTEM YAPISI

Çalışmamızda konsorsiyuma iletilen mesajlar kaybolmaması için kuyruk yapısında tutulmaktadır. Sistemi test ettiğimizde kullandığımız kuyruk yapısının teoride yapılan matematiksel hesaplamalarla ne kadar eşleştiği incelenir. Performansımızın teorik olarak hesaplanan değerlere ne kadar yakın olduğunu gözlemlemek ve normalde yüksek mobilitede kullanılmayan blok zincir gibi bir teknolojinin veri bütünlüğü katkısını kullanarak iyi bir performans sağlamak önemli bir katkı oluşturmaktadır.



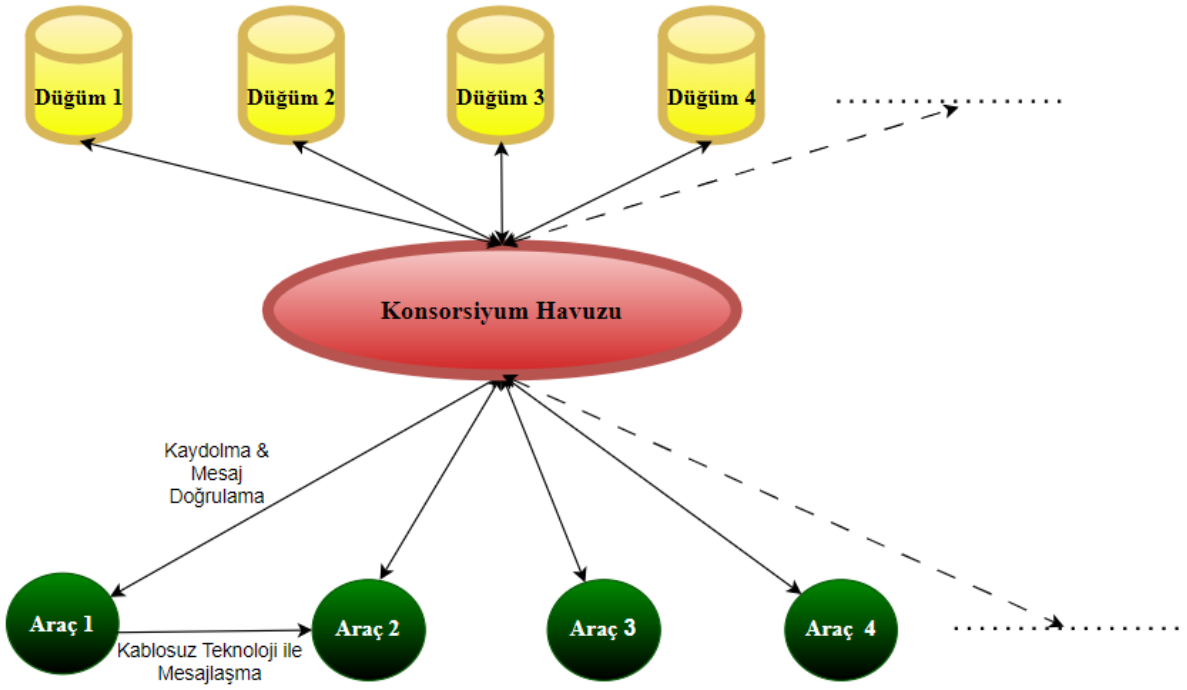
Şekil 3.1: Genel Şematik Gösterim.

Sistemimizin şematik görünümü Şekil 3.1'de görünmektedir. Burada da görüldüğü üzere Araçlar konsorsiyum havuzu üzerinden taleplerini iletirler. Sonrasında herhangi bir konsorsiyum düğümü iletilen talebi işler ve sonucunu ilgili araca iletir.

Şekil 3.2'de görüldüğü gibi genel sistem tasarımı düğümleri, konsorsiyum yapısını ve araçları içerir. Bu şekilde görülebileceği gibi konsorsiyum için düğümlerimiz var. Araçlar mesajlarını veya sisteme katılma isteklerini kendilerine en yakın düğüm üzerinden konsorsiyum havuzuna gönderebilirler. Sistemimizde 5, 7, 9 ve 11 düğüm için testler yapılmıştır. Bu test sonuçları bulgular bölümünde yer almaktadır.

Genel sistemin sözde kod parçası aşağıdaki gibidir:

```
main()
    if new:
        createVehicle(vehicle)
    if communication:
        verify(vehicle)
        createBlock(vehicle)
```



Şekil 3.2: Genel Sistem Tasarımı.

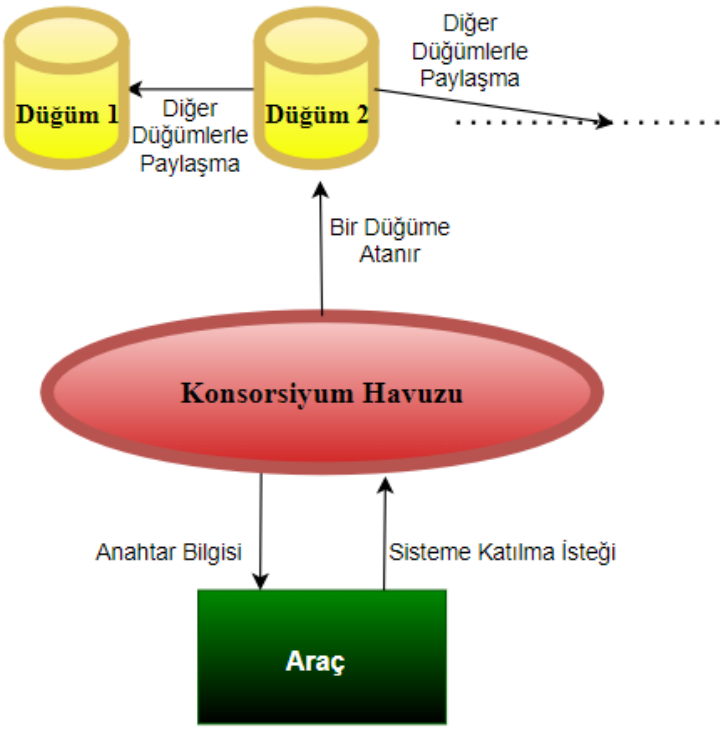
Şekil 3.3'de görüldüğü gibi, bir araç sisteme katılmak için konsorsiyum havuzu aracılığıyla sisteme katılma isteği gönderir. İlgili talep sonucunda işlem bir konsorsiyum düğümüne yönlendirilir ve aracın genel (public) ve özel (private) anahtarları üretilir. Üretilen anahtarlar araçla paylaşılır. Sisteme dahil edilen araç için üretilen anahtar bilgileri, diğer konsorsiyum düğümleri ile de paylaşılır.

3.2. SİSTEME KATILMA SÜRECİ

Önceki başlıklarda bahsedilen konsorsiyum düğümleri örneğin bir şehrin belirli noktalarına kapsama alanı düşünülerek yerleştirilen statik sunucular olarak da düşünülebilir. Bu sunucuların ve araçların internet bağlantısına sahip olduğu varsayılmaktadır. İnternet bağlantısı üzerinden iletişim kurarlar. İnternet bağlantısının daha hızlı olması ve kesinti olasılığının düşük olması göz önünde bulundurularak konumsal olarak iletişim kuracak araca yakın olan konsorsiyum düğümü üzerinden iletişim kurması sağlanmaktadır.

Sistemimizde Konsorsiyum havuzlu bir makine üzerinde bulunmaktadır. Bir şehir için yapıldığı düşünüldüğünde havuza gelen istekler şehirdeki düğümlere sıralı olarak gönderilir.

Şekil 3.3'de görüldüğü gibi bir araç, sisteme katılmak için konsorsiyum havuzu üzerinden sisteme katılma isteği göndermektedir. İlgili talep sonucunda aracın genel ve özel anahtarları oluşturulur. Oluşturulan anahtarlar araçla paylaşılır. Sisteme dahil edilen araç için üretilen anahtar bilgiler diğer konsorsiyum düğümleri ile paylaşılmaktadır.



Şekil 3.3: Aracın Sisteme Dahil Olması.

Sisteme dahil edilmek için kullanılan algoritmanın sözde kodu aşağıdaki yöntemlerden oluşmaktadır.

createVehicle(vehicle)
Node node = findNearestNode(vehicle.latitude, vehicle.longitude)
node.sendSystemEnrollRequest(vehicle)

Yukarıdaki sözde kod ile sisteme katılmak isteyen araç, konsorsiyum havuzuna istekte bulunur ve atanan bir düğüm üzerinden sisteme katılma isteği oluşturur.

sendSystemEnrollRequest(vehicle)
Generate PublicKey
Generate PrivateKey
Calculate Hash SHA256(vehicle, publicKey)
Add hash to address list map
Share Other Consortium Nodes

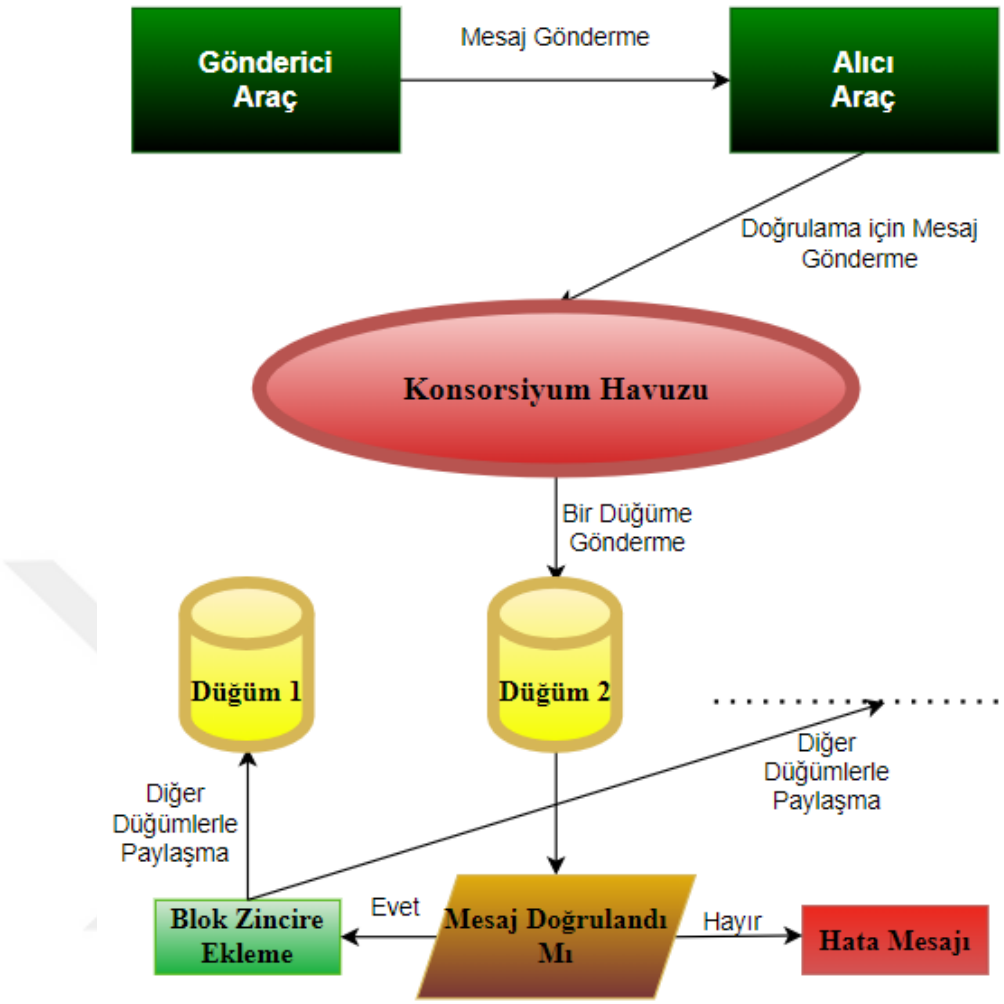
Yukarıdaki sözde kod ile oluşturulan sisteme dahil edilecek talep ile talebi oluşturan araca ait genel anahtar, özel anahtar ve hash oluşturulur. Oluşturulan hash karma adres listesine eklenir.

Anahtar üretimi algoritması aşağıdaki sırayla ilerler:

- p ve q olacak şekilde iki büyük asal sayı seçilir,
- n değeri p ve q kullanılarak hesaplanır, $n = pq$
- ϕ hesaplanır, $\phi(n) = (p-1)(q-1)$
- 1 ile ϕ arasında bir e ortak asal değer seçilir, $e, 1 < e < \phi(n)$
- ϕ ile mod işlemi yapılarak d hesaplanır, $de = 1\ (mod\ \phi(n))$
- n ve e kullanılarak Açık Anahtar oluşturulur (n,e),
- n ve d kullanılarak Kapalı Anahtar oluşturulur (n,d).

3.3. MESAJLAŞMA SÜRECİ

Şekil 3.4'te gösterildiği gibi, bir araç diğer araca bir mesaj gönderir. Gönderilen mesajı doğrulamak için doğrulamak isteyen konsorsiyum havuzu üzerinden uygun olan düğümlerden biriyle paylaşılır. Onay alması durumunda mesaj doğrulanır ve zincire eklenir, sonuç doğrulama isteyen araca gönderilir.



Şekil 3.4: Mesajlaşma Süreci.

Şekil 3.4'de görüldüğü gibi bir araç diğer bir araca mesaj göndermektedir. Gönderilen mesajı doğrulamak için konsorsiyum havuzuna yapılan istek, boşta kalan konsorsiyum düğümlerinden biriyle paylaşılır. Paylaşılan konsorsiyum düğümü onaylasa da onaylamasa da sonuç, doğrulama isteyen araca gönderilir. PoA'nın sistemi hızlandıran bir faktör olarak kullanılması sayesinde klasik blok zincir'de yer alan %51 onay beklentisi burada yoktur. Ayrıca kuyruk sayesinde veri kaybının da önüne geçilmektedir. Doğrulanma işlemi gerçekleşmezse bir hata mesajı görüntülenir. Doğrulanması durumunda blok zincirine eklenmek üzere diğer konsorsiyum düğümleriyle paylaşılır.

Sistemde blok oluşturma ile ilgili sözde kod parçaları aşağıdaki gibidir.

```
createBlock(node, message)
    if node.verify(message) is true
        Add Block to BlockChain
else
        error message
```

Sistemde işlemlerin doğrulanması ile ilgili sözde kod parçaları aşağıdaki gibidir.

```
verify(message)
    İf AdressListCheck(vehicle.message.senderHash) is not
exist
        return false (Unknown Vehicle)
    calculatedMerkleRoot = Calculate
MerkleRoot(vehicle.messages)
    İf merkleRootCheck(merkleRoot, calculatedMerkleRoot )
is false
        return false (Invalid Root)
    Calculate hash SHA256 (previousHash,
calculatedMerkleRoot , timestamp)
    İf calculatedHashCheck is false
        return false
    return true
```

Sistemde mesajlaşma sürecindeki adımlar şu şekildedir:

- Bir araca başka bir araca mesaj gönderir,
- Gönderici aracı doğrulamak için konsorsiyum havuzuna istekte bulunur,
- Mesaj konsorsiyum havuzuna gönderilir,
- Mesaj müsaitlik durumuna göre bir konsorsiyum düğümüne gönderilir,
- Bir düğüme gönderilen işlem kuyruğa eklenir,
- Mesaj doğrulanırsa onay cevabı gider
- Mesaj doğrulanır ise zincire eklenir

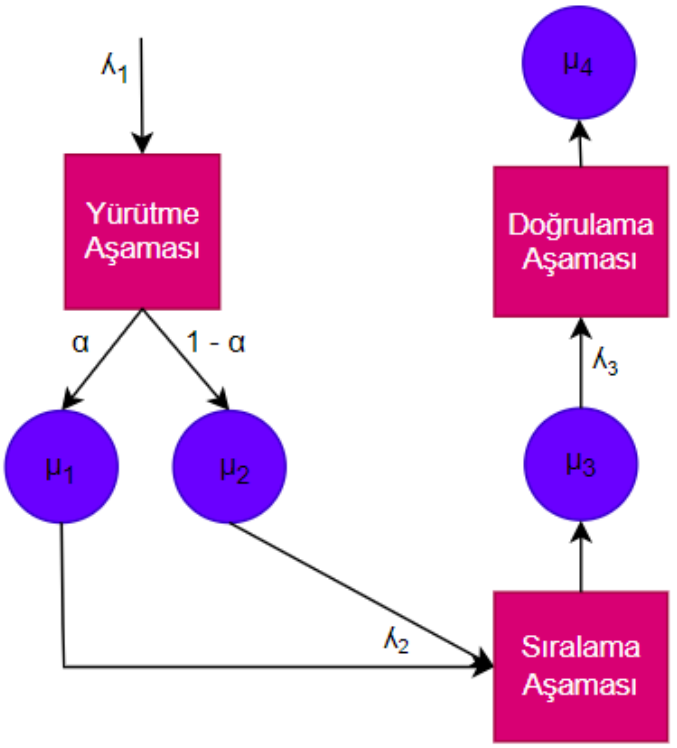
- Zincire eklenen blok bilgisi diğer konsorsiyum düğümleri ile paylaşılır

Doğrulaması talep edilen düğüm, sistemdeki konsorsiyum havuzuna doğrulama isteğinde bulunur. Doğrulama gerçekleşirse, mesaj zincire eklenir. Doğrulama işlemi sırasında öncelikle mesajı gönderen aracın adres listesinde yer alıp almadığına bakılır. Adres, adres listesinde yoksa, bilinmeyen bir araç hatası verilir.

Daha sonra merkleRoot hesaplanır ve hesaplanan değerin gerçekten zincirin merkleRoot değeri olup olmadığı kontrol edilir. Hesaplanan değer eşleşmezse geçersiz kök hatası verilir. Son olarak hash değeri hesaplanır ve hesaplanan hash değerinin doğruluğu kontrol edilir. Doğru değilse, geçersiz bir hash hatası verilir.

Yukarıda bahsedilen tüm kontrollerden geçen mesaj zincire eklenir.

3.4. PERFORMANS ÖLÇÜTÜ



Şekil 3.5: Kuyruk Modeli.

Zincire eklenecek blokların oluşturulacağı aşama 3 aşamaya ayrılmaktadır. Bunlar, Şekil 3.5'te görüldüğü gibi yürütme, sıralama ve doğrulama olarak sıralanmaktadır. Bu aşamalar, yürütme aşamasında konsorsiyum düğümüne ulaşmak için kuyruğa alınmadan önce geçtiği aşamadır. Sıralama aşaması, doğrulama süreci öncesinde sıralamanın yapıldığı aşamadır. Doğrulama aşamasında işlendiği düğümdeki zincire dahil edilip edilmeyeceğine ilişkin kararın verildiği aşamadır.

Konsorsiyum tipi blok zincirlerde, işlemler bir kuyruk ağında gerçekleştirilebilir. Bu kuyruk ağında işlemleri daha verimli hale getirmek için bazı öneriler bulunmaktadır. Bu önerileri ele aldığımızda süreçler 3 aşamaya ayrılmıştır. Bunlar yürütme, sıralama ve doğrulamadır. Bu aşamaların her biri için performans değeri, TPS (Transaction Per Second) ve işlem gecikmesi olarak tanımlanır. Örneğin, R rastgele bir sayı olduğu varsayılmaktadır. E beklenti fonksiyonu olarak tanımlanmaktadır. Bu durumda, rastgele bir zamandaki ortalama tepki süresi E[R] olarak adlandırılır. E[R] 3 aşamayı da içerir. Bu aşamalar E[Re], E[Ro] ve E[Rv] olarak adlandırılır. TPS, aşağıdaki formül 3.1'de hesaplanır. Tp değerleri TPS hesaplanırken kullanılır. *Ntrx* değeri işlem sayısını, Tp değeri işlem süresini temsil eder. Formül 3.1'de ortalama yanıt süresi hesaplanır. İlgili formüldeki N değeri konsorsiyumdaki üye sayısını, E[N] ise olasılık değerini temsil etmektedir. Son olarak, lambda değeri işlem varış oranı olarak tanımlanır.

$$TPS = N_{trx} / T_p \tag{3.1}$$

$$E[R] \tag{3.2}$$

Her aşama için hesaplanabilen işlem numaralarının toplamı E[N] değerini verir. Bu ifade formül 3.3'de yer almaktadır. Formül 3.4, 3.5 ve 3.6 sırasıyla E[Ne], E[No] ve E[Nv]'nin hesaplanmasını göstermektedir.

$$E[N] = E[N_e] + E[N_o] + E[N_v] \tag{3.3}$$

$$E[N_e] = \pi_e (I - \tau_e)^{-2} . 1_e \tag{3.4}$$

$$E[N_o] = \lambda_2/(\mu_3 - \lambda_2) \quad (3.5)$$

$$E[N_v] = \pi_v(I - \tau_v)^{-2}.1_v \quad (3.7)$$

Yukarıdaki formül 3.5, 3.6 ve 3.7'deki elementlerin karşılık gelen değerleri aşağıdaki formüllerde verilmiştir. Örnek olarak, bazı örnekler uygulama aşamasını göstermektedir. (Neuts'un oran matrisi[37]).

$$\tau_e = \lambda(\lambda \mathrm{I} - S_e - \lambda 1_e \beta_e)^{-1} \quad (3.8)$$

$$\beta_e = [\alpha \;\; 1-\alpha\,] \quad (3.9)$$

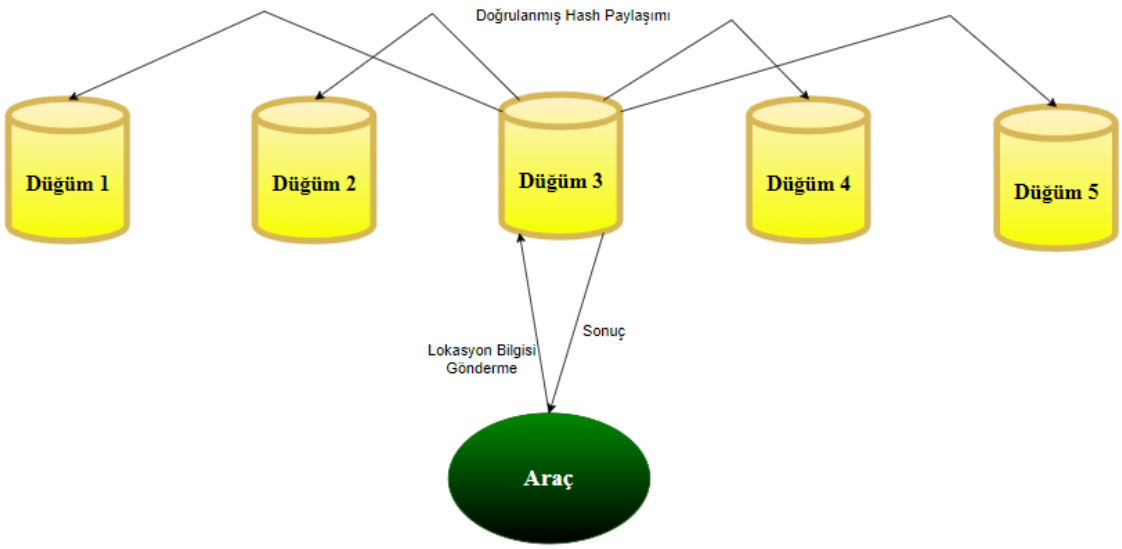
$$S_e = \begin{bmatrix} -\mu_1 & 0 \\ 0 & -\mu_2 \end{bmatrix} \quad (3.10)$$

$$1_e = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (3.11)$$

Formüllerde yer alan λ ve μ değerlerini şekil 3.4'de görünmektedir.

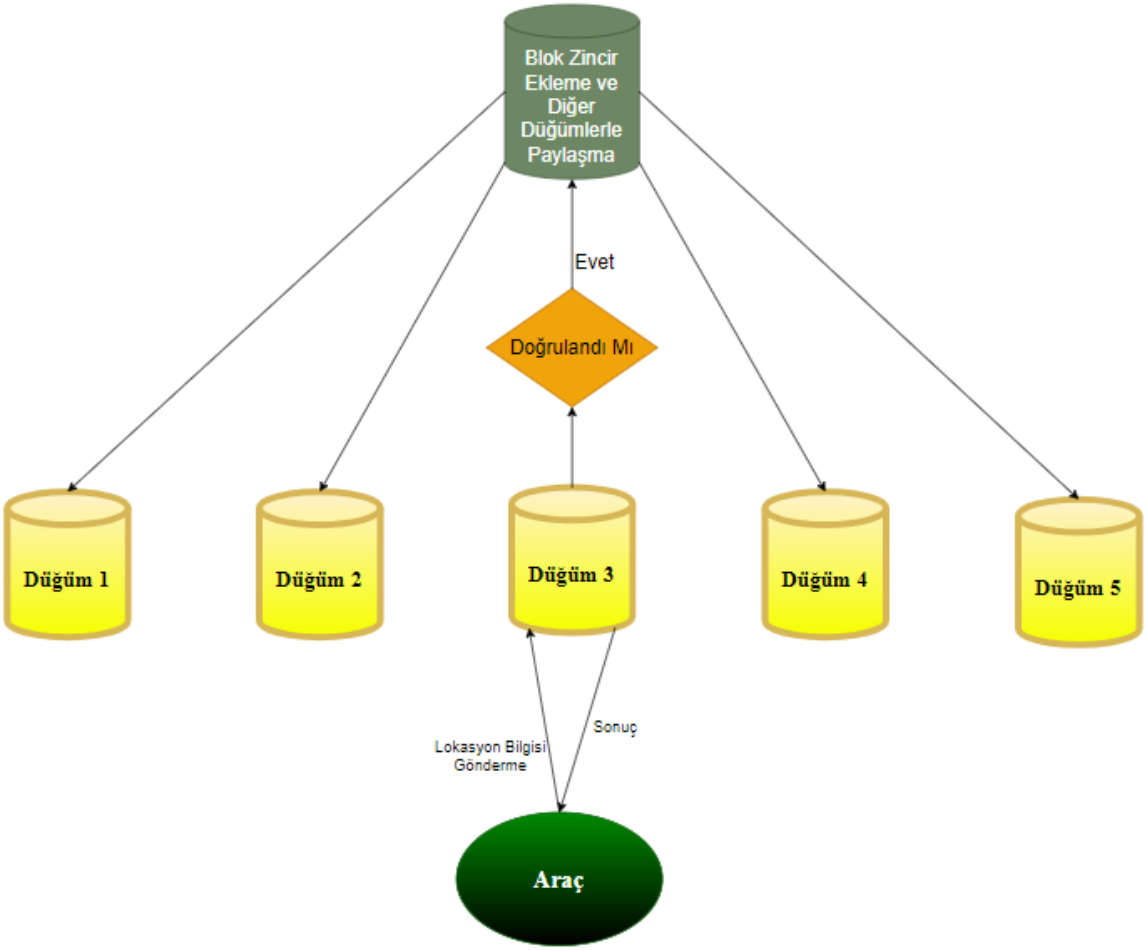
3.5. ARAÇ SOSYAL AĞI

Öncelikle sistemimizde araçların doğrulama ve iletişim süreçleri için gerekli altyapıya sahip olduğu varsayılmaktadır. Tüm araçların birbirleriyle iletişim kurabildiği kablosuz ağ teknolojilerinin var olduğu kabul edilmektedir. Ayrıca sisteme dahil olan tüm araçların konum bilgilerinin bulunduğu bölgesel sunucuya erişim sağlamak için tüm araçların internet bağlantısına sahip olduğu varsayılmaktadır. Bu nedenle, özgünlüğün sağlanması amacıyla genel ve özel anahtarları oluşturacak, yayınlayacak ve doğrulayacak bir ortak anahtar altyapı sağlayıcısının olduğu varsayılmaktadır.



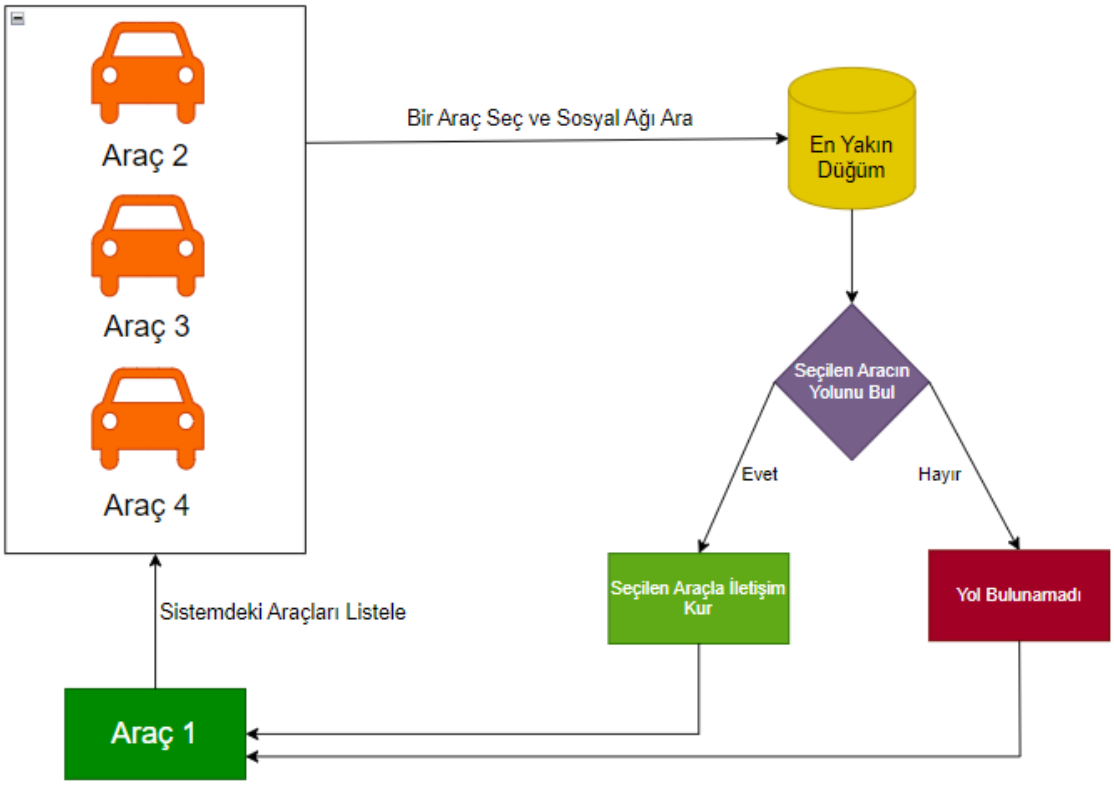
Şekil 3.6: Araç Sosyal Ağı Genel Yapısı.

Genel sistem mimarimiz Şekil 3.6'da gösterilmektedir. Örnek olarak konsorsiyumu oluşturan 5 düğüm bulunmaktadır. Herhangi birinden sisteme katılma talebi ile sistemimize araç eklenmektedir. Eklenen aracın bilgileri diğer konsorsiyum düğümleriyle de paylaşılmaktadır. Sisteme eklenen her araç için bir genel ve bir özel anahtar oluşturulur. Bu anahtarlar, ekleme sonucuyla birlikte araca yanıt olarak gönderilir.



Şekil 3.7: Araç Sosyal Ağı Blok Zincir Eklenmesi.

Şekil 3.7'de görüldüğü üzere araç sosyal ağında ilgili araç en yakındaki konsorsiyum düğümüne konum bilgilerini gönderir. Araç gönderdiği bilgideki araç yani gönderici hash bilgisi ile konsorsiyum düğümlerinden alınan tarafından doğrulanırsa yeni konum bilgisi zincire eklenir. Araç sosyal ağı için ikinci bir zincir kullanılmaktadır. Bunun sebebi ise daha sık gönderilecek konum bilgileri ile araçların haberleşmesi bilgilerinin birbirlerini bekletmesine sebep olmamasının istenmesidir. Benzer durum kripto para ödeme sistemlerinde de kullanılmaktadır.



Şekil 3.8: Araç Sosyal Ağı İletişim Süreci.

Araç sosyal ağında herhangi bir araç herhangi bir araçla iletişim kurmak isterse ve iletişim kurmak istediği araç ile kablosuz olarak yakınlığı bulunmuyorsa konsorsiyumdaki en yakın düğüme bir istek göndererek iletişim kurmak istediği araç ile herhangi bir bağının olup olmadığını sormaktadır. Eğer bağlantı var ise mesajlaşma sağlanır. Yoksa ise bağlantı bulunmadığı bilgisi verilmektedir. Şekil 3.8 bu durumu özetlemektedir.

Yukarıda bahsedilen yapının gerçekleşebilmesi için anlık konum bilgisi güncellenerek bağlı araçların kayıt altına alındığı blok zincirinde saklanmaktadır. Bu şekilde, bir aracın kaydının son konum bilgisi blok zincirine dahil edilir. Bloktaki bilgiler Şekil 3.9'daki bilgileri içermektedir. Bu bilgiler içerisinde yer alan gönderen araç hash bilgisi gönderen bilgisidir. Alıcı araç kimliği, menzil dışında olan ve listeden iletişim kurmak için seçilen aracı ifade eder. Aynı zamanda gönderen aracın zaman bilgisi (zaman damgası) ve o anki konumu gönderilir. Bağlı olan tüm araçlar konum bilgilerini anında blok zincir sunucusuna gönderdiği için, alıcı araç kimliği kullanılarak alıcı aracın konum bilgisi elde edilebilir. Aynı zamanda, blok zinciri

sunucusunda gönderen bilgisi ve anahtar bilgisi alınır. Ardından gönderilen şifreli konum bilgisinin kodu çözülebilir.

Şekil 3.9: Araç Sosyal Ağı İstek İçeriği.

Ayrıca gelen konum bilgisi ile blok zincirde bağlı aracı bularak konum bilgisini güncelleyen algoritmanın sözde kodu aşağıda verilmektedir.

```
setLocation(senderHash, locationInfo, privateKey)
        block = searchBlock(senderHash);
        locationText = decodeWithKey(privateKey, locationInfo);
        updateBlockLocation(block, locationInfo);
```

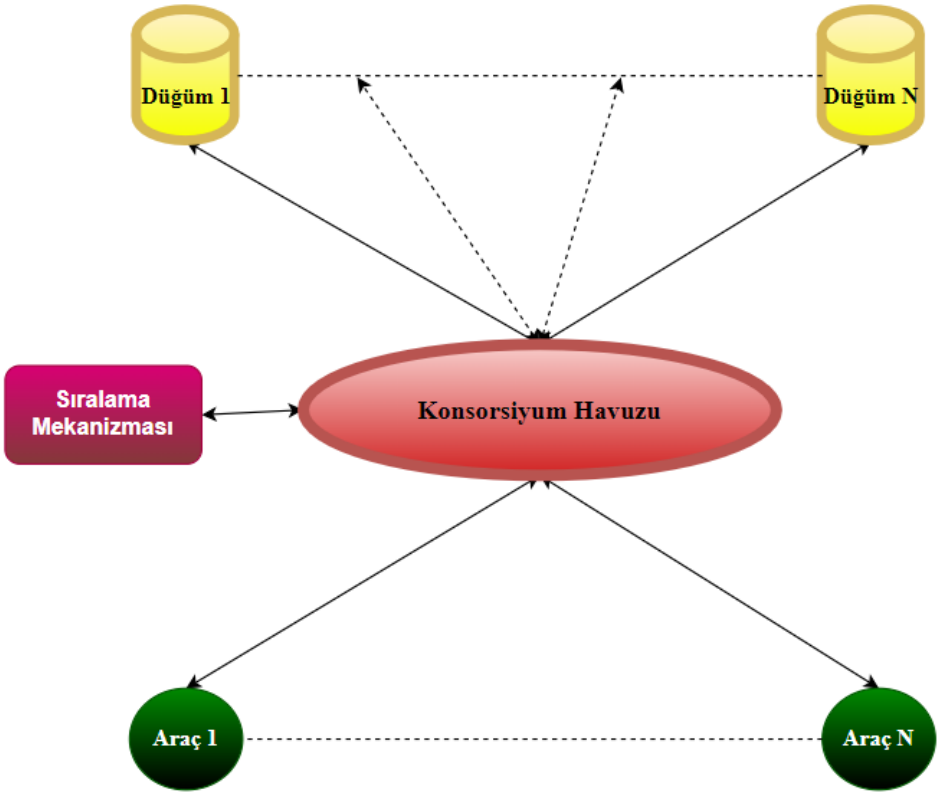
Yukarıdaki fonksiyon ile öncelikle blok zincirindeki bloğa erişilir ve ilgili bloktaki bilgiler kullanılarak konum bilgilerinin şifresi çözülmekte ve erişilmektedir. Ardından bloğun sahibi olan aracın konum bilgisi güncellenmektedir. Güncellenme işlemi aslında güncelleme değil ilgili aracın zincirin içerisinde en ileride yer alan konum kaydını ifade etmektedir.

Tüm bu yapıda iki blok zinciri vardır. Bu blok zincirlerinden biri bağlı araçların anahtarlarını ve son konum bilgilerini içerirken, diğer blok zinciri ise bağlı araçlar arasındaki mesajlaşmayı içermektedir. Bu iki blok zincirin tutulduğu yerler farklıdır. Blok zincirde, konum ve anahtar bilgileri içeren bir blok zinciri vardır. Bağlı araçlar arasındaki mesajlaşmayı içeren blok zincir, bağlı araçlarda saklanmaktadır.

Genel olarak bir araç, internet bağlantısı olan blok zincir tabanlı sistemimize bir istek göndererek kaydolmaktadır. Daha sonra kayıtlı araca genel ve özel anahtarlar verilmektedir. Bunlar hem mesajlaşma hem de konum bilgilerini paylaşmak için kullanılmaktadır. Bir araç, kapsamı dışında iletişim kurmak isterse, blok zincirden çektiği araçlar listesinden seçim yapar ve ilgili araca ulaşabilecek bir kablosuz ağ zinciri olup olmadığını blok zincirden sorgulamaktadır. Ulaşabileceği bir zincir bulursa iletişime geçmektedir. Bu iletişim için en önemli unsur, tüm sistemdeki araçları şifreleyerek konum bilgisini blok zincire göndererek blok zincirindeki konum bilgisinin anlık olarak güncellenmesidir.

4. BULGULAR

Önerilen model yöntem başlığı altında belirtilen mantıkta kullanılmaktadır. Araçlar arası iletişimde kullanılan veriler sentetik olarak üretilmekte ve test amaçlı kullanılmaktadır. Kullanılan sistem ağı şekil 4.1'de gösterilmektedir. Toplamda konsorsiyum için 5 düğüm içeren bir konsorsiyum örnek olarak kullanılmaktadır. Ayrıca her düğümde doğrulama için bir sertifika vardır. Bu düğümler arasında bir sıralama mekanizması kurulur. Her düğüm bir bilgisayara bir docker konteyneri olarak kurulur. Bu işlem bilgisayarda sanallaştırma ile gerçekleştirilmektedir. Diğer bir deyişle, her düğüm fiziksel olarak aynı makine üzerinde olmasına rağmen, ayrı adreslere sahip sanal cihazlardır. Bir önceki bölümde bahsedilen sözde kodların verildiği blok zincir algoritması her bir düğüme kurulur.

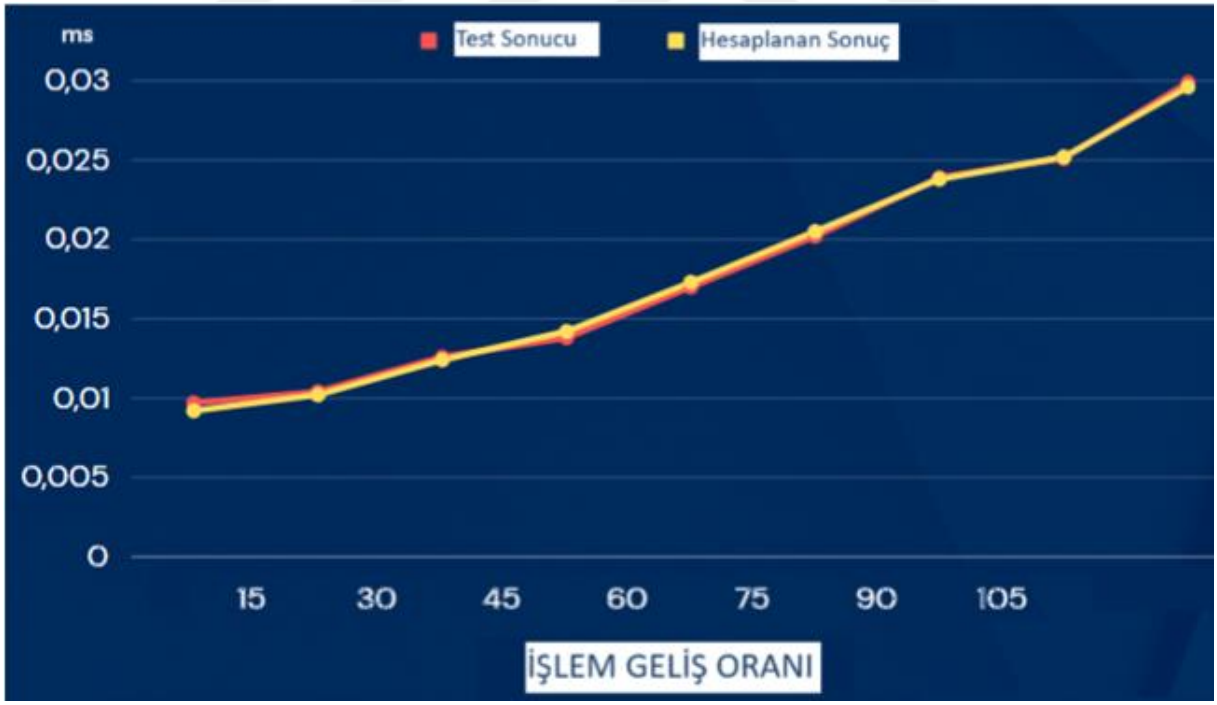


Şekil 4.1: Sistem Ağ Topolojisi.

Kullanılan fiziksel makine, 8 GB DDR4 RAM ile Intel(R) Core(TM) i5-5200U CPU'ya (2,2 GHz) sahiptir. İşletim sistemi Windows 10 64 bit işletim sistemidir. Her işlemin süresi, her aşamanın loglanan kayıtlarındaki işlem süreleri yazdırılarak elde edilir. Bu süreler üzerinden istatistiksel, kavramsal ve test sonuçları irdelenmektedir.

Örnek olarak hesaplanan değerler ve grafikleri verilen test değerleri 11 konsorsiyum düğümü içindir. Algoritmamız gereği düğüm sayısındaki artışın 11'e kadar çıkarılması olumlu sonuçlar verdiğini göstermektedir. Bu nedenle deneylerimiz arasında en iyi değerler olan 11'in grafikleri aşağıda gösterilmektedir. Düğüm sayısı arttıkça hesaplanan değerler elbette değişeceği için hesapladığımız düğüm sayısına göre grafikler verilmiştir. Ayrıca algoritmamızın doğası gereği konsorsiyum düğümü sayısı arttıkça bekleme süresi düşeceğinden sonuçlar düğüm sayısı arttıkça daha iyi olması beklenmektedir. Biz deneyimlediğimiz fiziksel bilgisayarın kapasitesini maksimum kullanacak düğüm sayısı 11 olduğu için 11 düğüm için olan sonuçlar sunulmaktadır.

4.1. YÜRÜTME AŞAMASI



Şekil 4.2: Yürütme Aşaması Test ve Hesaplanan Değer.

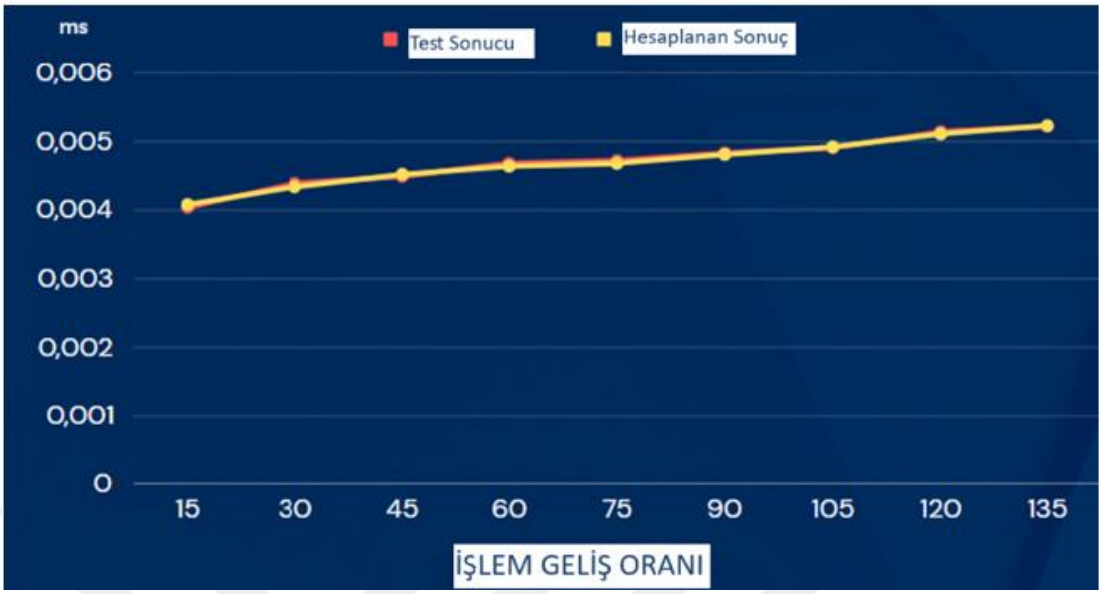
Hesaplanan ve test edilen süreler yürütme aşaması için bulgular kısmında ifade edildiği gibi hesaplanmaktadır. Şekil 4.2'deki grafik, işlem geliş oranı (Transaction Arrival Rate) ve ortalama yanıt süresi (Response Time) kullanılarak elde edilmektedir. Şekil 4.2 grafiği incelendiğinde işlem geliş oranı 20'den az olduğu durum dışında hesaplanan değerle sonuçlar örtüşmektedir. Örtüşmemenin sebebi oranın düşük olması ve grafiğin on binde birler seviyesinde olmasıdır. Bu hesaplamalarla sistemimizin verimi %90'ın üzerindedir.

4.2. SIRALAMA AŞAMASI

Şekil 4.3: Sıralama Aşaması Test ve Hesaplanan Değer.

Hesaplanan ve test edilen süreler sıralama aşaması için bulgular kısmında ifade edildiği gibi hesaplanmaktadır. Şekil 4.3'teki grafik, işlem geliş oranı ve ortalama yanıt süresi kullanılarak elde edilmektedir. Şekil 4.3 grafiği incelendiğinde işlem geliş oranı 20 ile 40 arasında olduğu durum dışında hesaplanan değerle sonuçlar örtüşmektedir. Örtüşmemenin sebebi oranın düşük olması ve grafiğin on binde birler seviyesinde olmasıdır. Örtüşmeyen durumlarda da sapma kabul edilebilir durumdadır. Bu hesaplamalarla sistemimizin verimi %95'in üzerindedir.

4.3. DOĞRULAMA AŞAMASI



Şekil 4.4: Doğrulama Aşaması Test ve Hesaplanan Değer.

Hesaplanan ve test edilen zamanlar doğrulama aşaması için bulgular kısmında ifade edildiği gibi hesaplanmaktadır. Şekil 4.4'deki grafik, işlem geliş oranı ve ortalama yanıt süresi kullanılarak elde edilmektedir. Ayrıca yine aynı şekilde görüleceği üzere işlem geliş oranları sayısı 20 ile 40 için tam olarak örtüşmemektedir. Bunun sebebi oranın düşük olması ve grafiğin on binde birler seviyesinde olmasıdır. İlgili verideki örtüşmeme miktarı da kabul edilebilir bir durumdadır. Sistemimizin verimi %90'ın üzerindedir.

4.4. DİĞER ÇALIŞMALARLA PERFORMANSA GÖRE KARŞILAŞTIRMA

Tablo 4.1'de seçilen çalışmalar kendi alanlarındaki en önemli çalışmalardır. Tablo 4.2'de görüldüğü üzere konsorsiyum tipi blok zincirlerin kullanımı bizim çalışmamızda da olduğu gibi oldukça nadirdir. Tabloda da belirttiğimiz gibi genel blok zinciri yavaş bir sistem olduğundan hareket kabiliyeti yüksek sistemler için pek uygun değildir. Özel blok zincirleri ise tek bir merkezi otorite tarafından yönetildikleri için güvenlik açısından riskler taşımaktadırlar. Ayrıca çoğu sistemdeki RSU'ların kullanımı, sistemlere ekstra maliyetler ve güvenlik riskleri eklediğinden dolayı çok maliyetlidir.

Tablo 4.1: Diğer Çalışmalarla Performansa Göre Karşılaştırma.

Referans	Blok Zincir	Ortalama Süre
[64]	Genel	221 ms
[65]	Özel	125.08 ms
[66]	Özel	39.585 ms
[67]	Özel	41.083 ms
Çalışmamız	Konsorsiyum	14.98 ms

Karşılaştırılan çalışmalarda kullanılan blok zincir türleri farklıdır. Aynı zamanda kurulan yapılar ve bunları zincire ekleme mantığı da farklılık göstermektedir. Ancak sistemimizin genel olarak kullanılan sistemin verdiği ortalama süre açısından iyi bir noktada olduğu görülmektedir. Çalışmamızda kullandığımız test işleminin geliş oranı (Transaction Arrival Rate) 70'tir. Bu tüm aşamalar için aynı şekilde kullanılmaktadır. Ayrıca eş zamanlı kullanılan mesaj sayısı da 100 olarak kabul edilmektedir. Daha önce de belirttiğimiz gibi algoritmamızdaki düğüm sayısını artırmak performansı artıracağından karşılaştırma tablosunda 5 düğümlü konsorsiyumun sonuçları yer almaktadır. Bunun 5 olmasının sebebi, en düşük düğüm sayısı olarak kullandığımız örnek sonuçlar elde ettiğimiz düğüm sayısının bu olmasıdır.

4.5. DİĞER ÇALIŞMALARLA TEORİK KARŞILAŞTIRMA

Tablo 4.2'de yer alan çalışmaların teorik olarak dezavantajları ile ilgili bilgler yer almaktadır. Aynı zamanda önerilen sistemin avantajları da aynı tabloda açıklanmaktadır.

Tablo 4.2: Diğer Çalışmalarla Teorik Karşılaştırma.

Referans	Blok Zincir	İşlem Düğümü	Konsensus	Sistemimize Göre Negatif Yanları
[11]	Genel	Her Düğüm	PoW	Genel Blok Zincir kullandığı ve PoW mekanizması kullandığı için oldukça yavaştır.
[59]	Genel	Block Manager	PoW	Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.
[68]	Konsorsiyum	RSU'lar	PBFT	RSU kullanımı nedeniyle uygulanması da maliyetlidir.
[69]	Genel	Her Düğüm	PoW	Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.
[70]	Genel	RSU'lar	Distributed Consensus	Genel Blok Zincir kullandığı için oldukça yavaştır. RSU kullanımı nedeniyle uygulanması da maliyetlidir.
[71]	Özel	CA	PoA	Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur.
[72]	Genel	RSU'lar	PoW	Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.
[73]	Genel	Vehicle Leader	PoW	Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.
[74]	Özel	RSU'lar	PoA	Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur. RSU kullanımı nedeniyle uygulanması da maliyetlidir.
[75]	Genel	RSU'lar	PoW	Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.

Tablo 4.2 (devam): Diğer Çalışmalarla Teorik Karşılaştırma.

[76]	Özel	CA	PoW	Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur. Ayrıca PoW oldukça yavaş bir fikir birliğine sahiptir.
Proposed Work	Konsorsiyum	Each Consortium Nodes	PoA	Her konsorsiyum düğümü karar mekanizmasında yer alır ve düğümlerin bir tanesinin onaylaması yeterlidir. Bu hız ve güvenlik açısından avantajlıdır.

[59]'da Genel blok zincir kullanılmaktadır. İşlem yapılan düğümler her yol kenarı birimlerinde yapılmaktadır. Konsensus mekanizması olarak PoW kullanılmaktadır. Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.

[64]'de Genel blok zincir kullanılmaktadır. İşlem yapılan düğümler her düğümde yapılmaktadır. Konsensus mekanizması olarak PoW kullanılmaktadır. Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.

[65]'de Konsorsiyum blok zincir kullanılmaktadır. İşlem yapılan düğümler yol kenarı birimlerinde yapılmaktadır. Konsensus mekanizması olarak PBFT kullanılmaktadır. RSU kullanımı nedeniyle uygulanması da maliyetlidir.

[66]'da Genel blok zincir kullanılmaktadır. İşlem yapılan düğümler her düğümde yapılmaktadır. Konsensus mekanizması olarak PoW kullanılmaktadır. Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.

[67]'de Genel blok zincir kullanılmaktadır. İşlem yapılan düğüm Blok Yöneticisinde yapılmaktadır. Konsensus mekanizması olarak PoW kullanılmaktadır. Genel Blok Zinciri ve PoW mekanizması kullandığı için oldukça yavaştır.

[70]'de Genel blok zincir kullanılmaktadır. İşlem yapılan düğümler her yol kenarı birimlerinde yapılmaktadır. Konsensus mekanizması olarak dağıtık konsensus kullanılmaktadır. Genel blok zincir kullandığı için oldukça yavaştır. RSU kullanımı nedeniyle uygulanması da maliyetlidir.

[71]'de Özel blok zincir kullanılmaktadır. İşlem yapılan düğüm merkezi bir otoritede yapılmaktadır. Konsensus mekanizması olarak PoA kullanılmaktadır. Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur.

[74]'de Özel blok zincir kullanılmaktadır. İşlem yapılan düğümler yol kenarı birimleridir. Konsensus mekanizması olarak PoA kullanılmaktadır. Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur. RSU kullanımı nedeniyle uygulanması da maliyetlidir.

[76]'da Özel blok zincir kullanılmaktadır. İşlem yapılan düğüm merkezi bir otoritedir. Konsensus mekanizması olarak PoW kullanılmaktadır. Sistemin karar mekanizması tek bir yere bağlı olduğundan güvenlik açısından sorunludur. Ayrıca PoW oldukça yavaş bir fikir birliğine sahiptir. Yukarıda seçilen çalışmalar kendi alanlarındaki en önemli çalışmalardır. Seçilen çalışmalarda görüldüğü gibi konsorsiyum tipi blok zincirlerin kullanımı oldukça nadirdir. Yukarıda da belirtildiği gibi Genel blok zinciri yavaş bir sistem olduğundan hareket kabiliyeti yüksek sistemler için pek uygun değildir. Özel blok zincirleri ise tek bir merkezi otorite tarafından yönetildikleri için güvenlik açısından riskler taşımaktadırlar. Ayrıca çoğu sistemdeki RSU'ların kullanımı, sistemlere ekstra maliyetler ve güvenlik riskleri eklediğinden dolayı oldukça maliyetlidir.

4.6. DÜĞÜM SAYISINA GÖRE KARŞILAŞTIRMA

Tablo 4.3: Düğüm Sayısına Göre Karşılaştırma.

Düğüm Sayısı	Yürütme Aşaması (Ortalama)	Sıralama Aşaması (Ortalama)	Doğrulama Aşaması (Ortalama)	Toplam Ortalama Bekleme Süresi
5	3.6 ms	8.6 ms	2.78 ms	14.98 ms
7	3.52 ms	8.51 ms	2.65 ms	14.68 ms
9	3.45 ms	8.38 ms	2.58 ms	14.41 ms
11	3.34 ms	8.25 ms	2.46 ms	14.05 ms

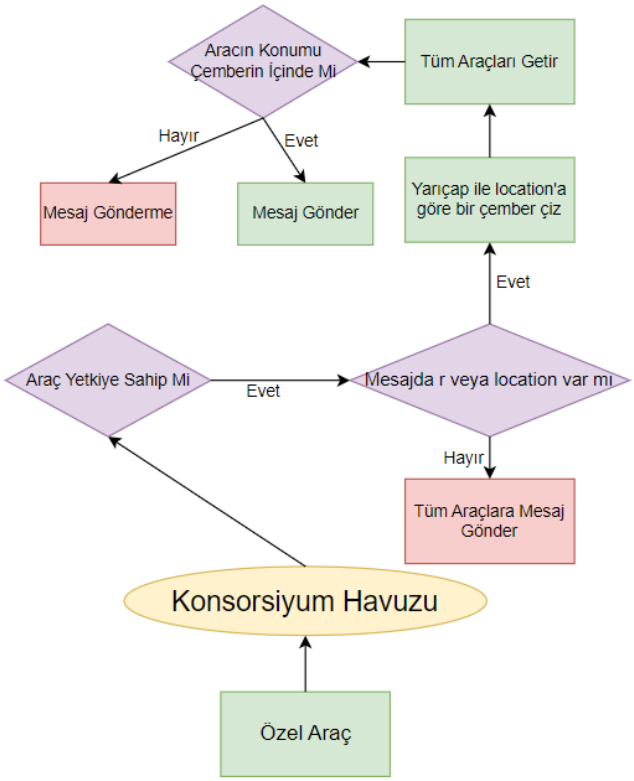
Sistemimiz düğüm sayısından bağımsız olarak iyi performans göstermektedir. Ancak test sonuçlarını incelendiğinde düğüm sayısı arttıkça mesaj trafiğini sabit tuttuğumuzda

sistemimizin hızlandığı ve ortalama bekleme süresinin azaldığı görülmektedir. Tablo 4.3'teki bilgilerde işlem varış hızı ve düğüm sayısına dayalı değerler görülmektedir. Çalışmamızda kullandığımız test işleminin varış oranı 70'tir.

4.7. GENEL MESAJ YAYINLAMA

Acil durumlarda veya sistemdeki belli bölgede bulunan araçlara veya tüm araçlara bir mesaj gönderilmek istendiğinde kullanılan senaryoya toplu mesaj senaryosu denmektedir. Bu durumda sistemde yer alan seçilen araçlara istenilen bilgi konsorsiyum havuzu üzerinden gönderilmektedir.

Genel mesaj yayınlama senaryosu Şekil 4.5'de görülmektedir. Özetlemek gerekirse sisteme kaydolan bazı araçlar tüm araçlara veya belli bir bölgeye mesaj yayınlama hakkına sahip olabilmektedir. Bu senaryo mevcut yapıya ek bir senaryodur. Bu isteği sadece sisteme dahil olurken bu yeteneğe sahip araçlar bileceği için konsorsiyum düğümlerinden ziyade genel sistemle alakalıdır.



Şekil 4.5: Genel Mesaj Yayınlama.

İşlem adımlarını sıralamak gerekirse:

- Sisteme dahil edilen araçlara mesaj yayınlama yetkisi verilir.
- Bu araçların oluşturulan hash bilgileri saklanır.
- Genel mesaj yayınlamak isteyen araç konsorsiyum havuzuna istekte bulunur.
- Gelen mesajın tipinin mesaj yayınlama isteği olup olmadığına bakılır.
- Gönderici araç hash bilgisinden ilgili aracın genel mesaj yayma yetkisine sahip olup olmadığı incelenir.
- Gelen mesajda yarıçap ve konum bilgileri varsa, mevcut konumu gelen konum ile yarıçap olacak şekilde çizilen çemberin arasında kalan sistemdeki araçlara genel mesaj gönderilir.
- Gelen mesajda yarıçap ve konum bilgileri yoksa tüm araçlara genel mesaj gönderilir.

Tüm bu adımlar için özel araçlar için sisteme eklerken sözde kod parçası aşağıdaki gibidir.

```
addSpecialVehicle(vehicle)
        Generate PublicKey
        Generate PrivateKey
        Calculate Hash SHA256(vehicle, publicKey)
        Add hash to address list map
```

Özel araçlar konsorsiyum havuzuna istekte bulunduğunda çalışan sözde kod parçası aşağıdaki gibidir.

```
sendGeneralMessageRequest(senderHash, message)
    if checkPriority(senderHash)
        if message has radius
            sendAreaMessage(message)
        else
            sendAllVehicle(message)
    else
        has no priority error
```

Tüm araçlara mesaj göndermeye yarayan sözde kod aşağıdaki gibidir.

```
sendAllVehicle(message)
    List<Vehicle> vehicles = getAllVehicleHash(addressListMap)
    for(vehicle:vehicles)
        sendMessage(vehicle)
```

Belirlenen bölgedeki araçlara mesaj göndermeye yarayan sözde kod parçası aşağıdaki gibidir.

```
sendAreaMessage(message)
List<LocationInfo> areaList = createLocationInfoList(message.radius,
                              message.locationInfo)
List<Vehicle> vehicles = getAllVehicleHash(addressListMap)
for(vehicle:vehicles)
        for(locationInfo:areaList)
                if locationInfo include vehicle
                        send message
```

5. TARTIŞMA VE SONUÇ

Sonuç olarak bu çalışmada araçlar arası iletişimde blok zincir kullanılarak güvenli bir model oluşturulmaya çalışılmaktadır. Bu güvenli modelin güvenlik kısmı, verilerin konsorsiyum blok zinciri ile genel ve özel anahtarlar kullanılarak imzalanmasıyla gerçekleştirilmektedir. Güvenli bir şekilde iletişim kurarken yüksek hareket kabiliyetine sahip bir araç gibi bir unsurdaki performansı iyi değerlendirmek için konsorsiyum blok zinciri ve yetki kanıtı konsensüs algoritması kullanılmaktadır. Test sonuçlarında görüldüğü gibi iletişim oldukça hızlı ve verimli bir şekilde gerçekleşmektedir. Performans değeri yazılım araçları ve matematik formülleri ile hesaplanmakta ve değerler çok küçük sapmalarla örtüşmektedir. Blok zincir kullanımı, eğer doğru algoritmalar tercih edilmez ve klasik haliyle kullanılırsa araçlar arası iletişimde önemli gecikmelere ve iletişim sorunlarına neden olabilmektedir. Bu durum gerçek zamanlı uygulamalarda kritik bir endişe kaynağı olabilmektdir. Bu sorunun çözümünde yukarıdaki test sonuçları bölümünde görüldüğü gibi konsorsiyum tipi blok zincir kullanımı ve PoA konsensüs algoritmasının kullanılması ile aşılabilmektedir. Bu çalışma teorik olarak hesaplanan değerler ile sistemin test edildiği değerlerin karşılaştırılması yoluyla gerçekleştirilmektedir. Ayrıca literatürde hesaplanan değerlerin bulunduğu bazı çalışmalarla da kıyaslanmaktadır.

Çalışmamızda gerçekleştirdiğimiz algoritmik ve yazılımsal geliştirmeler modüler yapısı sayesinde birçok senaryoyu denememize olanak sağlamaktadır. Literatürde yer alan çalışmalardaki kaynak kod eksikliği projelerle yapılacak kıyaslamada en önemli zorluktur. Özetle çalışmamızda performans ve güvenlik açısından en kullanışlı olan Konsorsiyum blokzincirini yine performansı düşünerek yetki kanıtı algoritması ile kullanılmaktadır. Burada ek olarak bir havuz yapısı ve kuyruk eklenerek veri kaybının da önüne geçilmektedir.

Güvenlik olarak blokzincire ekleme aşamasında her araç için birer genel ve özel anahtar oluşturulmaktadır. Bu sayede mesaj gönderen ve alan araçların iletişimini sadece kendileri anlayabilmektedir. Ayrıca blokzincirde yer alan veri bütünlüğünün korunması da sağlanmaktadır. Blokzincir teknolojisinin doğasında bu durum yer almaktadır. Kullanılan onay mekanizması ve her defterde bu bilginin saklanıyor olması bu durumu sağlamaktadır. Çalışmamızdaki güvenli modelde yer alan güvenlik unsuru veri bütünlüğünü ifade etmektedir.

Son olarak test edebildiğimiz diğer çalışmalardan gayet iyi sonuç elde edilmektedir. Elbette bunun en önemli sebebi farklı bir blokzincir türü ve konsensüs algoritmasının kullanılmasıdır. Ek olarak da kuyruk yapısının sisteme entegre edilmiş olması sayesinde iyi sonuçlar elde edilmektedir.

6. GELECEK ÇALIŞMALAR

Gelecek çalışmalarımızda literatürede yeni yeni giren hibrit blokzincir uygulamaları üzerine çalışmayı hedeflemekteyiz. Hibrit algoritmaların güvenlik ve performans açısından daha iyi olup olmadığını inceleyeceğiz. Çalışmamızda konsorsiyum düğümlerinin güvenli olduğunu kabul etmekteydik. Bu kabulün üzerine giderek sistemin farklı bir blokzincir yapısında en azından aynı performans seviyesinde olup olmadığını tespit etmeye çalışacağız.

Ayrıca kısa vadede konsorsiyum düğümlerindeki metriklere performansın yanında güvenlik saldırılarının eklenmesi de hedeflenmektedir.

KAYNAKLAR

[1]. Sultan, K., Ruhi, U., Lakhani, R., 2018, Conceptualizing Blockchains: Characteristics and Applications, *11th IADIS International Conference on Information Systems*, 49–57.

[2]. Anascavage, R., Davis, N., 2018, Blockchain Technology: A Literature Review, *Innovation Law & Policy eJournal*, pp.1-5.

[3]. Ferrer, B.R., Mohammed, W.M., Lastra, J.L.M., Villalonga, A., Beruvides, G., Castaño, F., Haber, R.E., 2018, Towards the adoption of cyberphysical systems of systems paradigm in smart manufacturing environments, *In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, Porto, Portugal, 18–20 July 2018; IEEE: New York, NY, USA, 2018; pp. 792–799.

[4]. Fernandez-Carames, T.M., Fraga-Lamas, P., 2019, A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories, *IEEE Access*, 7, 45201–45218.

[5]. Dorri, A., Kanhere, S.S., Jurdak, R., 2017, Towards an optimized blockchain for IoT, *In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Pittsburgh, PA, USA, 18–21 April 2017; IEEE: New York, NY, USA, 2017; pp. 173–178.

[6]. Rahman, A., Islam, M.J., Rahman, Z., Reza, M.M., Anwar, A., Mahmud, M.A.P., Nasir, M.K., Noor, R.M., 2020, DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. *IEEE Access*, 8, 209594–209609.

[7]. Loklindt, C., Moeller, M.P., Kinra, A., 2018, How blockchain could be implemented for exchanging documentation in the shipping industry, *In International Conference on Dynamics in Logistics*, Springer: Berlin/Heidelberg, Germany, pp. 194–198.

[8]. Mettler, M., 2016, Blockchain technology in healthcare: The revolution starts here, *In Proceedings of the 2016 IEEE 18th International Conference on eHealth Networking*,

Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; IEEE: New York, NY, USA, pp. 1– 3.

[9]. Akhter, A., Ahmed, M., Shah, A., Anwar, A., Zengin, A., 2021, A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET, *Sustainability*, 13, 400.

[10]. Wang, C., Shen, J., Lai, J.F., Liu, J., 2020, B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs, *IEEE Trans. Emerg. Top. Comput.*, pp. 1-5.

[11]. Shrestha, R., Bajracharya, R., Shrestha, A.P., Nam, S.Y., 2020, A new type of blockchain for secure message exchange in VANET, *Digit. Commun. Netw.*, 6, 177–186.

[12]. Kulathunge, A., Dayarathna, H., 2019, Communication framework for vehicular ad-hoc networks using Blockchain: Case study of Metro Manila Electric Shuttle automation Project, *In Proceedings of the 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, Colombo, Sri Lanka, 28 March 2019; IEEE: New York, NY, USA, pp. 85–90.

[13]. Taghizadeh, H., Solouk, V., 2015, A novel MAC protocol based on cooperative master-slave for V2V communication, *In Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, Prague, Czech Republic, 9–11 July 2015; IEEE: New York, NY, USA, pp. 1–5.

[14]. Lai, C., Ding, Y., 2019, A Secure Blockchain-Based Group Mobility Management Scheme in VANETs, *In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC)*, Changchun, China, 11–13 August 2019; IEEE: New York, NY, USA, pp. 340–345.

[15]. Javaid, U., Aman, M.N., Sikdar, B., 2019, DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts, *In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, 28 April–1 May 2019; IEEE: New York, NY, USA, pp. 1–5.

[16]. Ali, I., Gervais, M., Ahene, E., Li, F., 2019, A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs, *J. Syst. Archit.*, 99, 101636.

[17]. Lu, Z., Wang, Q., Qu, G., Liu, Z., 2018, Bars: A blockchain-based anonymous reputation system for trust management in vanets, *In Proceedings of the 2018 17th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 1–3 August 2018; IEEE: New York, NY, USA, pp. 98–103.

[18]. Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z., 2018, A privacy-preserving trust model based on blockchain for VANETs, *IEEE Access*, 6, 45655– 45664.

[19]. Zhang, X., Chen, X., 2019, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, *IEEE Access*, 7, 58241–58254.

[20]. Malik, N., Nanda, P., Arora, A., He, X., Puthal, D., 2018, Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, *In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 1–3 August 2018; IEEE: New York, NY, USA, pp. 674–679.

[21]. Lin, C., He, D., Huang, X., Kumar, N., Choo, K.K.R., 2020, BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks, IEEE *Trans. Intell. Transp. Syst.*, 1-5.

[22]. Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X., 2008, An efficient identitybased batch verification scheme for vehicular sensor networks, *In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 13–18 April 2008; IEEE: New York, NY, USA, pp. 246–250.

[23]. Rongxing, L., Xiaodong, L., Xuemin, S., 2010, SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks, *In Proceedings of the IEEE INFOCOM*, San Diego, CA, USA, 15– 19 March 2010; pp. 1–9.

[24]. Shao, J., Lin, X., Lu, R., Zuo, C., 2015, A threshold anonymous authentication protocol for VANETs, *IEEE Trans. Veh. Technol.*, 65, 1711–1720.

[25]. Azees, M., Vijayakumar, P., Deboarh, L.J., 2017, EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks, *IEEE Trans. Intell. Transp. Syst.*, 18, 2467–2476.

[26]. Li, H., Pei, L., Liao, D., Chen, S., Zhang, M., Xu, D., 2020, FADB: A FineGrained Access Control Scheme for VANET Data Based on Blockchain, *IEEE Access*, 8, 85190–85203.

[27]. Salem, A.H., Abdel-Hamid, A., El-Nasr, M.A., 2016, The case for dynamic key distribution for PKI-based VANETS, *arXiv*, pp. 1-5.

[28]. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018, On blockchain and its integration with IoT Challenges and opportunities, *Future Generation Computer Sysems.*, 88, 173–190.

[29]. Glaser, F., 2017, Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis, *HICSS*, pp. 1-5.

[30]. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564.

[31]. Nakamoto, S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, [Ziyaret Tarihi: 31 Mayıs 2024].

[32]. Beck, R., 2018, Beyond Bitcoin: The Rise of Blockchain World, *Computer*, 51(2), 54–58.

[33]. Tama, B.A., Kweka, B.J., Park, Y., Rhee, K.H., 2017, A critical review of blockchain and its current applications, *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 109–113.

[34]. Ferrer, B.R., Mohammed, W.M., Lastra, J.L.M., Villalonga, A., Beruvides, G., Castaño, F., Haber, R.E., 2018, Towards the adoption of cyber-physical systems of systems paradigm in smart manufacturing environments, *In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, Porto, Portugal, 18–20 July 2018; IEEE: New York, NY, USA, pp. 792–799.

[35]. Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X., 2008, An efficient identity-based batch verification scheme for vehicular sensor networks, *In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 13–18 April 2008; IEEE: New York, NY, USA, pp. 246–250.

[36]. Li, H., Pei, L., Liao, D., Chen, S., Zhang, M., Xu, D., 2020, FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain, *IEEE Access*, 8, 85190–85203.

[37]. Leiding, B., Memarmoshrefi, P., Hogrefe, D., 2016, Self-managed and blockchain-based vehicular ad-hoc networks, *In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, Heidelberg, Germany, 12–16 September 2016; pp. 137–140.

[38]. Shah, A.S., Ilhan, H., Tureli, U., 2019, RECV-MAC: A novel reliable and efficient cooperative MAC protocol for VANETs, *IET Commun. 2019*, 13, 2541–2549.

[39]. Yang, F., Tang, Y., 2014, Cooperative clustering-based medium access control for broadcasting in vehicular ad-hoc networks, *IET Commun. 2014*, 8, 3136–3144.

[40]. Woo, R., Han, D.S., 2012, A cooperative MAC for safety-related road information transmission in vehicular communication systems, *In Proceedings of the 1st IEEE Global Conference on Consumer Electronics 2012*, Tokyo, Japan, 2–5 October 2012; IEEE: New York, NY, USA, pp. 672–673.

[41]. Zhang, L., Jin, B., Cui, Y., 2014, A concurrent transmission enabled cooperative MAC protocol for vehicular ad hoc networks, *In Proceedings of the 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS)*, Hong Kong, China, 26–27 May 2014; IEEE: New York, NY, USA, 2014; pp. 258–267.

[42]. Zhou, T., Sharif, H.; Hempel, M., Mahasukhon, P., Wang, W., Ma, T., 2010, A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks. *IEEE J. Sel. Areas Commun.*, 29, 72–82.

[43]. Zhang, J., Zhang, Q.; Jia, W., 2008, VC-MAC: A cooperative MAC protocol in vehicular networks, *IEEE Trans. Veh. Technol.*, 58, 1561–1571.

[44]. Bharati, S., Zhuang,W., 2016, CRB: Cooperative relay broadcasting for safety applications in vehicular networks, *IEEE Trans. Veh. Technol.*, 65, 9542–9553.

[45]. Halpin, H., Piekarska, M., , 2017, Introduction to Security and Privacy on the Blockchain, *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1–3.

[46]. Hawlitschek, F., Notheisen, B., Teubner, T., 2018, The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, *Electronic Commerce Research Application,* 29, 50–63.

[47]. Zhao, J.L., Fan, S., Yan, J., 2016, Overview of business innovations and research opportunities in blockchain and introduction to the special issue, *Finance Innovation*, 2(1), 28.

[48]. Nath, I., 2016, Data Exchange Platform to Fight Insurance Fraud on Blockchain, *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 821–825.

[49]. Lewis, A., 2015, *So, You Want to Use a Blockchain for That ?*, https://www.coindesk. com/want-use-blockchain/, [Ziyaret Tarihi: 9 Ekim 2018].

[50]. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaria, V., 2018, To Blockchain or Not to Blockchain: That Is the Question, *IT Professional*, 20(2), 62–74.

[51]. Buterin, V., 2015, *On Public and Private Blockchains*, *Ethereum Blog Crypto renaissance salon*, https://blog.ethereum.org/ 2015/08/07/on-public-and-private-blockchains/, [Ziyaret Tarihi: 22 Ekim 2022].

[52]. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Das, G., 2018, Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems, *IEEE Consumer Electronics Magazine*, 7(4), 6–14.

[53]. Jindal, V., Bedi, P., 2016, Vehicular Ad-Hoc Networks- Introduction, Standards, Routing Protocols and Challenges, *International Journal of Computer Science Issues*, 13, 44-55.

[54]. Abbasi, I.A., Shahid Khan, A., 2018, A Review of Vehicle to Vehicle Communication Protocols for VANETs in the Urban Environment, *Future Internet 2018*, 10, 14.

[55]. Demba, A., Möller, D.P.F., 2018, Vehicle-to-Vehicle Communication Technology, *In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT)*, Rochester, MI, USA, 3–5 May 2018; pp. 0459–0464.

[56]. Zhu, H., Li, M., 2013, *Studies on Urban Vehicular Ad-hoc Networks SpringerBriefs*, in Computer Science, DOI: 10.1007/978-1-4614-8048-8_1.

[57]. Sheikh, M. S., Liang, J., Wang, W., 2019, A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs), *Sensors*, Basel, Switzerland, 19(16), 3589. https://doi.org/10.3390/s19163589.

[58]. Wu, X., Subramanian, S., Guha, R., White, R., Li, J., Lu, K., Bucceri, A., Zhang, T., 2013, Vehicular Communications Using DSRC: Challenges, Enhancements, and Evolution. Selected

Areas in Communications, *IEEE Journal on Selected Areas in Communications*, 31(9), pp. 399-408.

[59]. Kargl, F., Schoch, E., Wiedersheim, B., Leinmuller, T., 2008, Secure and efficient beaconing for vehicular networks, *Proc. Fifth ACM International Workshop on VehiculAr Inter-NETworking*, pp. 82–83.

[60]. Dorri, A., Steger, M., Kanhere, S., Jurdak, R., 2018, BlockChain: A Distributed Solution to Automotive Security and Privacy, *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119-125.

[61]. Wood, G., 2014, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf, [Ziyaret Tarihi: 22 Eylül 2017].

[62]. Aoun, A., 2019, *Blockchain for Electric Vehicle Charging*, https://blockchainjournaldotblog.wordpress.com/2019/12/05/blockchain-for-electric-vehicle-charging/, [Ziyaret Tarihi: 31 Mayıs 2024].

[63]. Buccafurri, F., Lax, G., Musarella, L., Russo, A., 2023, An Ethereum-based solution for energy trading in smart grids, *Digital Communications and Networks*, 9(1), pp. 194-202.

[64]. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L., 2017, ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid, Spain, pp. 468-477.

[65]. Chen, S., Zhang, J., Shi, R., Yan, J., Ke, Q., 2018, A Comparative Testing on Performance of Blockchain and Relational Database: Foundation for Applying Smart Technology into Current Business Systems. In: Streitz, N., Konomi, S. (eds) Distributed, Ambient and Pervasive Interactions: Understanding Humans, *DAPI 2018*, vol 10921.

[66]. Yan, T., Chen, W., Zhao, P., Li, Z., Liu, A., Zhao, L., 2019, Handling Conditional Queries on Hyperledger Fabric Efficiently, *In: Cheng, R., Mamoulis, N., Sun, Y., Huang, X. (eds) Web Information Systems Engineering – WISE 2019*, vol 11881.

[67]. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung,, 2019, A Permissioned Blockchain-Based System for Verification of Academic Records, *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Canary Islands, Spain, pp. 1-5.

[68]. C. Chen, J. Wu, H. Lin, W. Chen, Z. Zheng, 2019, A secure and efficient blockchainbased data trading approach for Internet of vehicles, *IEEE Trans. Veh. Technol. 68*, 9110–9121.

[69]. A. Mostafa, 2019, A general framework for detecting malicious vehicles, *J. Commun. 14*, 356–362.

[70]. A.S. Khan, K. Balan, Y. Javed, S. Tarmizi, J. Abdullah, 2019, Secure trust-based blockchain architecture to prevent attacks in VANET, *Sensors 19*, 4954.

[71]. N. Malik, P. Nanda, X. He, R. Liu, 2019, Trust and reputation in vehicular networks: a smart contract-based approach, *in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, IEEE, pp. 34–41.

[72 M. Baza, M. Nabil, M.M.E.A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, M. Abdallah, 2020, Detecting sybil attacks using proofs of work and location in VANETs, *IEEE Trans. Dependable Secure Comput*. 1–1.

[73]. M. Wagner, B. McMillin, 2018, Cyber-physical transactions: a method for securing VANETs with blockchains, *in: 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, IEEE, pp. 64–73.

[74]. M. Li, J. Weng, A. Yang, J.-N. Liu, X. Lin, 2019, Toward blockchain-based fair and anonymous ad dissemination in vehicular networks, *IEEE Trans. Veh. Technol.*, 68, 11248–11259.

[75]. D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang, 2019, A traceable blockchain-based access authentication system with privacy preservation in VANETs, *IEEE Access*, 7, 117716–117726.

[76]. A. Patel, N. Shah, T. Limbasiya, D. Das Vehiclechain, 2019, Blockchain-based vehicular data transmission scheme for smart city, *in: 2019 IEEE International Conference on Systems*, IEEE, 2019, pp. 661–667.

EKLER

Sisteme doğrulama işlemi için gelen istek örneği

{

senderHash:0vXvZhT45gXtMwT/2bx5ZvKMsVnGxDiYquEhoKWOQSE=,

timestamp:1705678083,

message:ada22e01db7c11797167b746bdf44af99d26bbce

}

Araç Sosyal Ağı bir aracın bir araçla sosyal ağ kurmak için sisteme gönderdiği istek örneği

{

senderHash:0vXvZhT45gXtMwT/2bx5ZvKMsVnGxDiYquEhoKWOQSE=,

receiverId:5,

timestamp:1717439283,

locationInfo:{

latitude:41.28428016335474,

longitude:29.37971177621671

}

}

Araç Sosyal Ağı bir aracın konum bilgisini sisteme göndermesi örneği

{

vehicleId:12,

timestamp:1704295683,

locationInfo:{

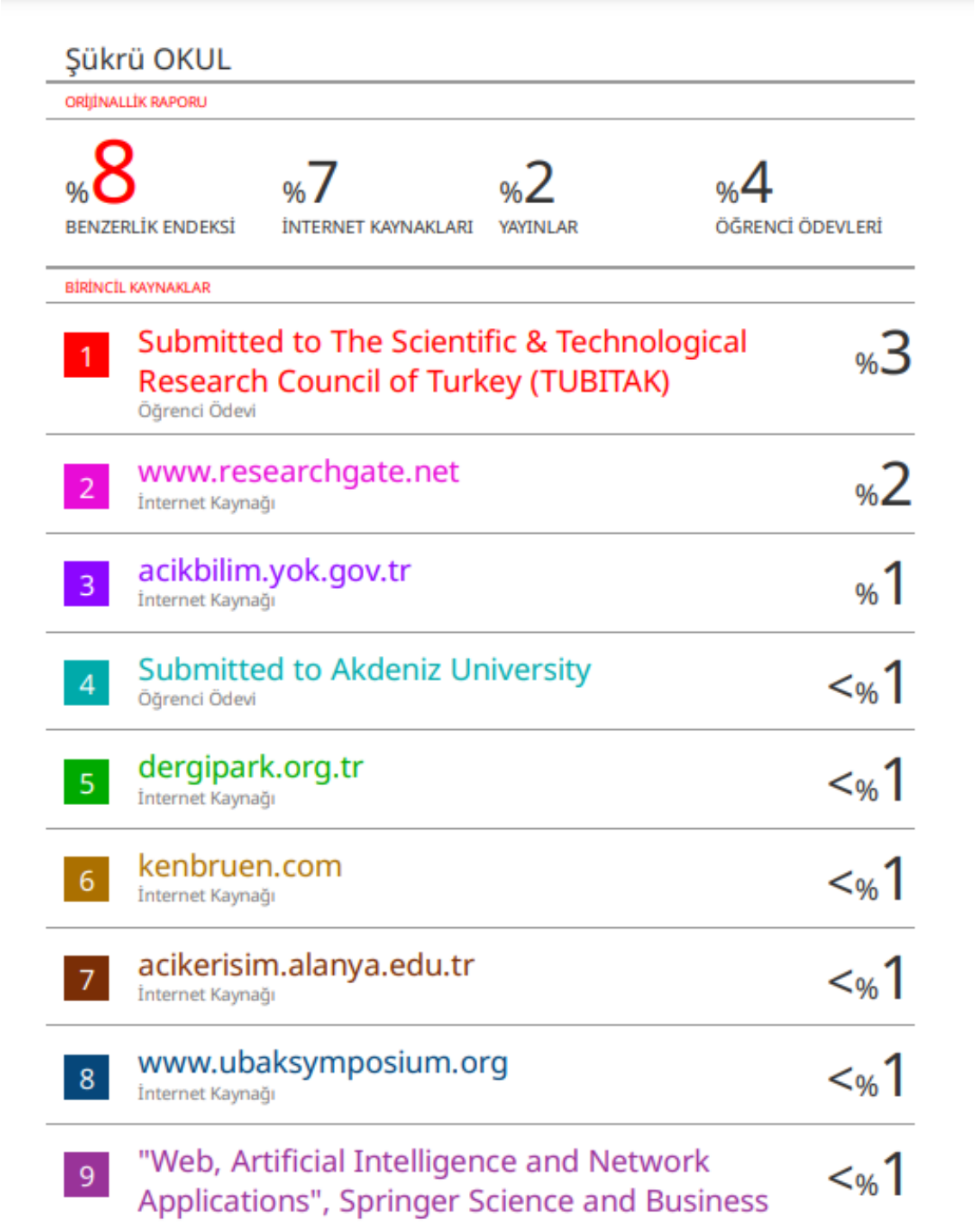
latitude:41.05506639094764,

longitude:28.916712538901987

}

}

İNTİHAL RAPORU İLK SAYFASI



Şükrü OKUL

ORİJİNALLİK RAPORU

%8	%7	%2	%4
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	%3
2	www.researchgate.net İnternet Kaynağı	%2
3	acikbilim.yok.gov.tr İnternet Kaynağı	%1
4	Submitted to Akdeniz University Öğrenci Ödevi	<%1
5	dergipark.org.tr İnternet Kaynağı	<%1
6	kenbruen.com İnternet Kaynağı	<%1
7	acikerisim.alanya.edu.tr İnternet Kaynağı	<%1
8	www.ubaksymposium.org İnternet Kaynağı	<%1
9	"Web, Artificial Intelligence and Network Applications", Springer Science and Business	<%1