AUSUD | BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ | JITSA

Araştırma Makalesi

Motorlu kara taşıtlarında güvenli ve güvenilir veri yönetim modeli

Suat Onur[1],*, Mehmet Tektaş[2], İlyas Özer[3], Ufuk Çelik[4], Emrah Dönmez[5], Caner Pense[2]

1Akıllı Ulaşım Sistemleri ve Teknolojileri, Lisansüstü Eğitim Enstitüsü, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye
2 Ulaştırma Mühendisliği, Mühendislik ve Doğa Bilimleri Fakültesi, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye
3 Bilgisayar Mühendisliği, Mühendislik ve Doğa Bilimleri Fakültesi, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye
4 Yönetim Bilişim Sistemleri, Ömer Seyfettin Uygulamalı Bilimler Fakültesi, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye
5 Yazılım Mühendisliği, Mühendislik ve Doğa Bilimleri Fakültesi, Bandırma Onyedi Eylül Üniversitesi, Bandırma, Türkiye
*Correspondence: suatonur@balikesir.edu.tr

DOI: 10.51513/jitsa.1644011

Özet: Kişisel ve ticari ulaşım için yaygın olarak kullanılan motorlu kara taşıtlarının üretiminden hurdaya ayrılmasına kadar geçen süreçte çeşitli kurum ve kuruluşlar tarafından toplanan ve saklanan önemli bilgiler bulunmaktadır. Bu bilgilerin kayıt altına alınması, denetim ve takip işlemlerini kolaylaştırmanın yanında, sürücü ve araçların güvenliğini sağlamak, trafik akışını düzenlemek, çevre kirliliğini azaltmak ve araç sahipleri ve sürücüleri çeşitli risklere karşı korumak gibi Akıllı Ulaşım Sistemlerinin temel hedeflerine hizmet eder. Ancak, araçlarla ilgili işlemlerde rol alan birçok resmi ya da özel kurumun kendi merkezi veri yönetim sistemlerine sahip olmasından kaynaklanan tek nokta hatası, kurumlar arası iş birliğinin yetersizliği, verilerin kayıt altına alınmasındaki zorluklar bazı sorunların ortaya çıkmasına sebep olabilmektedir. Bu sorunlar içerisinde özellikle ikinci el araç pazarında aracın geçmişine ait bilgilere ulaşmadaki zorluklar, kaza geçmişi ve bakım-onarım kayıtlarının yetersizliği, sigorta dolandırıcılığı, hile ve veri manipülasyonu ön plana çıkmaktadır. Bu makalede, araçlarla ilgili verilerin depolanması, yönetimi ve takibini daha verimli ve güvenli bir şekilde yapabilmek için Hyperledger Fabric özel-izinli blokzincir teknolojisi ile özel dağıtık dosya depolama (Private InterPlanetary File System, IPFS) teknolojisinin entegrasyonundan oluşan bir veri yönetim modeli önerilmiştir. Araçlarla ilgili işlemlerde kurumlar arası iş birliğinin daha şeffaf, güvenli ve güvenilir bir şekilde gerçekleştirilmesi hedeflenmektedir. Ayrıca araçlarla ilgili çeşitli verilerin depolanması ve yönetilmesi için geniş kapsamlı, ölçeklenebilir ve paylaşımlı bir altyapı oluşturmak amaçlanmıştır. Önerilen blokzincir ağ modeli araçlarla ilgili kurumsal hizmetlerin dijitalleştirilmesine, kâğıt tabanlı belge kullanımın azaltılmasına, iş ve işlem süreçlerinin sadeleştirilmesine ve maliyetlerin azaltılmasına katkı sağlayacağı gibi kurumlar arasında iş birliğini sağlama, iş akış süreçlerini ve veri yönetim modellerini daha güvenli ve güvenilir hale getirme noktasında yeni bir perspektif oluşturmakta ve gelecekte kamusal hizmetlerin daha fazla dijitalleşmesi ve şeffaflaşması için örnek teşkil etmektedir.

Anahtar Kelimeler: Blokzincir, araç yaşam döngüsü, araç veri yönetimi, dağıtık depolama, IPFS.

Secure and reliable data management model in motor vehicles

Abstract: The lifecycle of motor land vehicles, spanning from production to disposal, involves the collection and storage of critical data by various public and private institutions. Efficient management of this data is essential for achieving the core objectives of Intelligent Transportation Systems, including enhancing road safety, optimizing traffic flow, reducing environmental impact, and protecting stakeholders from fraud and security risks. However, the fragmentation of data across multiple

ORCID: 0000-0002-2265-0640, 0000-0001-9564-8069, 0000-0003-2112-5497, 0000-0003-3063-6272, 0000-0003-3345-8344, 0000-0003-2187-2193
Received 20.02.2025; Received in revised form 11.03.2025; Accepted 11.03.2025

centralized systems, coupled with limited inter-institutional collaboration, presents significant challenges. These challenges are particularly evident in the second-hand vehicle market, where issues such as inaccessible vehicle history, incomplete accident and maintenance records, insurance fraud, and data manipulation undermine transparency and trust. This paper proposes a secure and efficient data management framework that integrates Hyperledger Fabric permissioned blockchain technology with InterPlanetary File System (IPFS) based distributed storage. The proposed model aims to enhance data integrity, streamline vehicle-related processes, and foster secure and transparent collaboration among stakeholders. By providing a scalable and interoperable infrastructure, the framework facilitates secure data sharing, minimizes reliance on paper-based documentation, optimizes administrative workflows, and reduces operational costs. The adoption of this blockchain-based model is expected to contribute to the digital transformation of institutional vehicle services while establishing a robust foundation for the future expansion of transparent and secure public service infrastructures.

Keywords: Blockchain, vehicle lifecycle management, vehicle data integrity, decentralized storage, IPFS.

ORCID: 0000-0002-2265-0640, 0000-0001-9564-8069, 0000-0003-2112-5497, 0000-0003-3063-6272, 0000-0003-3345-8344, 0000-0003-2187-2193
Received 20.02.2025; Received in revised form 11.03.2025; Accepted 11.03.2025

1. Giriş

Sayıları düzenli olarak artan motorlu kara taşıtları (makalede araç kelimesi kullanılacaktır), birçok dijital teknolojiyle donatıldığı gibi, elektrikli, otonom ve bağlantılı araç teknolojilerinin kullanımıyla ortaya çıkan bilgi miktarı ve çeşitliliği de büyük oranda artmaktadır. Birçok dijital teknoloji ile donatılmış araçların veri yönetimi ve güvenliği konusu, gittikçe daha önemli ve karmaşık hale getirmektedir. Veri miktarındaki ve çeşitliliğindeki bu artış, veri yönetimi konusunda güvenlik, gizlilik, paylaşım ve depolamada çeşitli zorluklar ve problemler oluşturmaktadır. Bu bilgilerin kayıt altına alınması ve yönetimi, kullanıcı-araç-altyapı-merkez arasında çok yönlü veri alışverişi ile izleme, ölçme, analiz ve kontrol sağlamanın yanında (Tektaş, Korkmaz, & Erdal, 2016), sürücü ve araçların güvenliğini sağlamak, trafik akışını düzenlemek, çevre kirliliğini azaltmak ve araç sahipleri ve sürücüleri çeşitli risklere karşı korumak gibi Akıllı Ulaşım Sistemlerinin temel hedeflerine hizmet etmektedir.

Çoğu ülkede olduğu gibi Türkiye'de de araçlarla ilgili gerçekleştirilen işlemlerde kamu ve özel çeşitli kurumlarla iş birliği yapılması gerekmektedir. Üretim bilgileri, tescil ve ruhsat bilgileri, teknik muayene kayıtları, sigorta bilgileri, bakım onarım kayıtları, kullanım geçmişi, kaza kayıtları, trafik ihlal ve ceza kayıtları gibi birçok konu ve kapsamda tutulan bu kayıtlarda resmi ya da özel çeşitli kurumlar rol almaktadır. Ancak kurumlar arasındaki güvensizlikler, kişisel bilgilerin ifşasına neden olabilecek siber güvenlik zafiyetlerinden ve sorumluluklarından kaçınmak gibi nedenlerle kısıtlı miktarda bilgi alışverişi ve paylaşımı yapılabilmektedir. Kurumlar arası bilgi paylaşımının tam anlamıyla halen dijital ortamlarda yapılamaması neticesinde kâğıt tabanlı belge kullanımına devam edilmektedir. Örneğin, araç alım-satım ve tescil işlemlerinde çeşitli kâğıt tabanlı belge ve bilgiler istenmekte ve ıslak imza onayları kontrol edilerek işlemler yapılabilmektedir (ARTES Bilgi Sistemleri, 2018). E-devlet uygulamaları birçok kurum arasında iş birliğinin ve güvenin sağlanmasında, belge ve bilgilerin doğrulanmasında güvenilir üçüncü taraf olarak önemli bir rol üstlenmiştir. Ancak bu durum birçok işlemde tek nokta hatası ve darboğaz oluşturabilmektedir.

Kurumlar arası veri paylaşımında genellikle hassas verilerin ifşa edilme riski nedeniyle güvensizlik hakimdir. Kurumlar arasında güvene dayalı bir iş birliği ve bilgi paylaşımının yapılması için genellikle üçüncü bir tarafa ihtiyaç duyulur. Bu durum da merkezi bir yapılanma oluşturur. Kurumsal bilgi paylaşımına yönelik kullanılan ağ sistemleri genellikle sunucu-istemci bağlantı modeliyle çalışan merkezi sistemlerdir ve bilgiye erişim, Evrensel Kaynak Konumu (URL) yöntemi ile internet üzerindeki tek sunucu tarafından sağlanmakta ve kontrol edilmektedir. Bu nedenle merkezi yapıda tutulan veriler tek hata noktasına karşı savunmasızdır ve hizmet reddi saldırısı için potansiyel hedef konumundadır (Elisa, Yang, Chao, & Cao, 2023). Kurumların merkezi sistemleriyle ilgili önemli risklerden diğeri de yetkisini kötüye kullanan kurum personeli tarafından veri manipülasyonun yapılabilmesidir. Bu risklere karşı blokzincir teknolojisine dayalı merkezi olmayan veri depolama sistemlerini kullanmak izlenebilirlik ve inkar edilemezlik sağladığı için de önerilmektedir (Athanere & Thakur, 2022).

Literatürde, araçlarla ilgili çeşitli konu ve kapsamdaki bilgilerin kayıt altına alınmasında ve takip ve yönetimindeki zafiyetler ve eksikler nedeniyle ortaya çıkan birçok problem için blokzincir tabanlı çözüm önerileri ve uygulamaların sayısında artış gözlenmektedir. Çoğunlukla ele alınan problemler; ikinci el araç pazarındaki güvensizliğin temel nedeni olarak gösterilen araç geçmişine ait kayıtların olmaması veya yetersizliği (Baumann, Zavolokina, & Schwabe, 2021; Zafar, Hassan, Mohammad, Al-Ahmadi, & Ullah, 2022), aracın kaza geçmişi ve bakım-onarım kayıtlarına erişmedeki zorluklar (Akçi, 2016; Dayı & Hasanoğlu, 2023) , çalıntı araçların (Das, Banerjee, Ghosh, Biswas, & Bashir, 2021) ya da şasi ve motor numarası değiştirilen araçların satışa sunulması (Leila Benarous, Benamar Kadri, Ahmed Bouridane, & Elhadj Benkhelifa, 2021) , ağır hasarlı araçların hurdaya ayrılması gerektiği halde yolsuzluk yapılarak yeniden satışa sunulması (Brousmiche, Heno, Poulain, Dalmieres, & Ben Hamida, 2018), kilometre sayacı sahtekarlığı (Abbade et al., 2020; Car-Pass, 2022; Chanson, Bogner, Wortmann, & Fleisch, 2017; Holler, Barth, & Fuchs, 2019), kurumlar arası veri paylaşımının yetersizliği, kurumsal güç çekişmeleri, veri güvenliği ve veri kalitesindeki sorunlar (Schwabe, 2019) üzerinde birçok çalışma yapılmıştır. Ancak yapılan çalışmaların büyük bir kısmı sadece belirli problemlerin çözümü için gerekli olan verilerin depolama ve yönetiminde blokzincir tabanlı çözümler önermiş ve uygulamalar geliştirmişlerdir. Önerdiğimiz model geniş kapsamlı birçok verinin depolanması için bir altyapı oluşturmaktadır. Böylece yukarıda bahsi geçen birçok sorunun çözümünde önemli katkılar sağlanması hedeflenmektedir.

Önerilen model merkezi sistemlere ait sorunları önlemek için gizliliği ve bütünlüğü koruyan merkezi olmayan bir veri yönetim çerçevesi sunmaktadır. Blokzincir ve temel bileşeni olan Dağıtık Defter Teknolojisi (DLT) ile IPFS teknolojisi veri güvenliğini artıran merkezi olmayan sistemlerdir. Hyperledger Fabric blokzincir teknolojisinin sağladığı çok kanallı yapının avantajlarıyla birlikte özel IPFS teknolojisinin entegrasyonu sayesinde birçok kurumun ortak bir platform üzerinde iş birliği yapabilmesi mümkündür. Bu sistemde veriler tek sunucuda değil, dağıtılmış çok sayıdaki sunucuda mutabakat mekanizması ile güncellenerek ve doğrulanarak tutulmaktadır.

Önerilen modelde temel amaç, araçların trafiğe çıktığı ilk tescil tarihinden hurdaya ayrılana kadar gerçekleştirilen çeşitli işlemlere ait bilgilerinin blokzincir ve IPFS teknolojileri kullanılarak her araç için tanımlanan benzersiz kimlik bilgisi ile zaman damgalı kayıt altına alınması, depolanması ve gerektiğinde istenilen bilgilere erişilebilmesini sağlamaktır.

Bu yenilikçi yaklaşım hem araç sahiplerinin hem de yetkili resmi veya özel kuruluşların bir aracın geçmişine ilişkin bilgilere tek bir kaynaktan erişebilmelerini sağlayacaktır. Aracın geçmişine ilişkin değişmez kayıtların ve kanıtların varlığı sadece şeffaflığı sağlamakla kalmaz, aynı zamanda sistemin denetlenebilirliğini ve güvenilirliğini artırır. Bu verilere erişim, yetkilendirme ve izinlere dayalı olarak düzenlenerek sahtekarlık ve aldatma gibi potansiyel sorunlar da azaltılabilir.

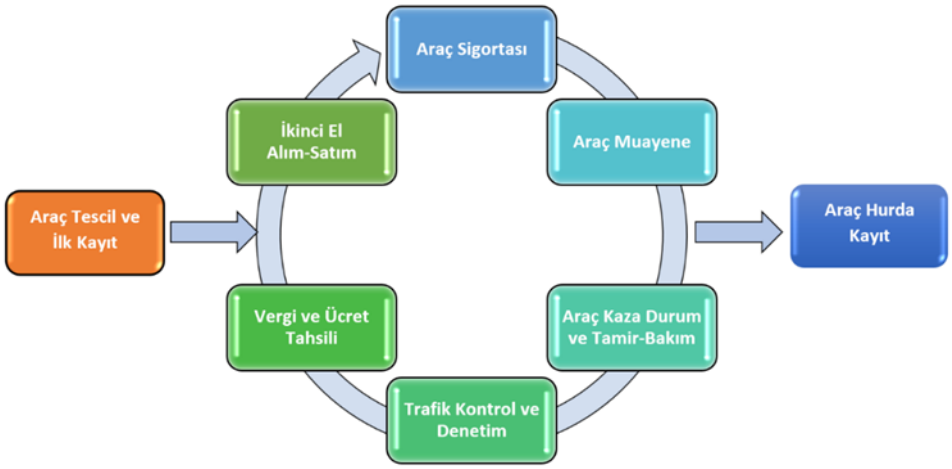
Önerilen modelin uygulanmasında öngörülen faydalar aşağıda özetlenmiştir;

- Birçok kuruluşun merkezi yapılarıyla ilgili tek nokta hatası riskleri ortadan kaldırılarak, araçlarla ilgili tutulan kayıtların bütünlüğünün, erişilebilirliğinin ve değişmezliğinin garanti altına alınmasını sağlayacaktır.
- Araçlara ait işlem geçmişlerine her istendiğinde kesintisiz bir şekilde ulaşılabilirliğin mümkün olması; bakım onarım kayıtlarının ve yedek parça kullanımlarının takip altına alınmasında, kilometre sayacı sahtekarlıklarının, hurdaya ayrılmış güvensiz araçların yeniden kullanıma sunulmasının engellenmesinde, ikinci el araç pazarındaki bilgi eksikliğinden kaynaklanan güvensizliklerin giderilerek kullanılmış araçların satış fiyatlarının daha doğru belirlenmesinde, hırsızlık, dolandırıcılık gibi zararlı faaliyetlerin önlenmesinde önemli katkılar sağlayacaktır.
- Ortak bir platform üzerinde birçok kurumun güvenli bir şekilde iş birliğiyle veri paylaşımı yapması, kâğıt tabanlı belge ve kimlik doğrulama ihtiyacını ortadan kaldırarak işlemlerle ilgili iş akış yöntemlerinin değişmesini sağladığı gibi maliyetlerin düşürülmesini, daha az insan gücü kullanımı ve zaman tasarrufu sağlayacaktır.
- Adli ve yasal takip gerektiren durumlarda, ilgili kurumların kanıt hükmündeki güvenilir bilgi ve belgelere erişimi daha kolay hale getirilerek, adli süreçlerin hızlanması ve denetim ve takip işlemlerindeki maliyetlerin azaltılmasında önemli katkılar sağlayacaktır.

2. Araçlardaki Veri Çeşitliliği ve Önemi

Akıllı Ulaşım Sistemlerinde, bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşması, dijital ortamlarda aktarılan, paylaşılan ve depolanan veri hacmini önemli ölçüde artırmıştır. Bu verilerin önemli bir kısmı, akıllı ulaşımda hareketliliğin en önemli bileşenlerinden olan araçlarla ilgilidir. Araçlarla ilgili üretilen bilginin yönetiminde resmi ve özel pek çok kurum görev almaktadır. Bu kurumların her biri kendi özel hedeflerine ve sorumluluklarına göre bilginin toplanması, işlenmesi ve depolanması süreçleri için kendi bilgi yönetim sistem ve teknolojilerini, kendi veritabanı, yazılım ve donanım kaynaklarını kullanmaktadır. Bu durumda aracın sahibi dahi kendi aracına ait kayıt altına alınan bilgilerin sahibi olamadığı gibi bu bilgilere erişimi de kolay değildir.

Araçların ilk tescil kaydı ile trafiğe çıktığı andan itibaren hurdaya ayrılana kadarki süreç içerisinde gerçekleştirilen birçok işleme ait kayıtların tutulması birçok problemin çözümü için oldukça önemlidir. Aracın yaşam döngüsüne ait çoğu zaman periyodik olarak tekrarlanan işlemlerin sınıflandırılmış veri çeşitliliği Şekil 1'de verilmiştir.



Şekil 1. Araçların yaşam döngüsündeki sınıflandırılmış işlemler.

Türkiye'de araçların yaşam döngüsü içerisinde zorunlu olarak tutulması gereken kayıtlarda; aracın ilk tescil işlemleri ile ikinci el araç alım-satım işlemlerinde Noterler Birliği, trafik ihlal ve denetim işlemleri ile kaza yönetimi Emniyet Genel Müdürlüğü Trafik Başkanlığı, araç muayene işlemlerinde TÜVTÜRK, zorunlu trafik sigortası ile kaza hasar ödeme ve takip işlemlerinde birçok sigorta kuruluşları, araç tamir, bakım ve servis hizmetlerinde birçok özel kuruluş, vergi ve HGS/OGS otomatik geçiş ücretlendirmeleri ve takibinde resmi ve özel kuruluşlar görev almaktadır. Bu kurumların her biri kendi sorumluluklarıyla ilgili bilgiler için kendilerine ait bilgi yönetim sistem ve teknolojilerini kullanmaktadır. Bu kurumların bir kısmı e-devlet uygulamaları ile belirli seviyede, sınırlı miktarda bilgi paylaşımı yapabilmektedir. A. Mahmutoğlu ve ark. (2012) "Trafik Sorununa Bir Çözüm Önerisi: Trafik İzleme Başkanlığı" isimli çalışmasında, bilgi ve iletişim teknolojilerinin sağladığı imkânlar ile her araçla ilgili her türlü verinin kurulacak Trafik İzleme Başkanlığı kurumuna ait merkezi bir sistemde tutulması önerilmektedir. Böylece tek merkezde tutulan verilerin işlenmesi ve analizi ile pek çok problemin çözülebileceği detaylı bir şekilde ele alınmaktadır. Daha geniş kapsamlı olarak M.Tektaş ve ark. (2016) tarafından önerilen Trafik Kontrol Merkezi yerine Ulaşım Kontrol Merkezinin kurularak ulaşımdaki tüm aktörlerden gelecek verilerin yönetilmesi ve değerlendirilmesi için merkezi bir sistem oluşturulmasının önemi vurgulanmıştır (Tektaş et al., 2016).

Günümüzde araçlarda kullanılan son teknoloji sistemler sayesinde aracın durumu ve kullanımı ile ilgili pek çok bilgi elde edilebilmektedir. Örneğin bir trafik kazası anında araç hızının veya emniyet kemeri kullanım bilgisinin tespit edilmesi ve bu bilgilerin inkâr edilememesinin sağlanması, sorumluların tespitinin doğru yapılması ve benzeri durumlara ait işlemlerin kayıt altına alınması büyük önem taşımaktadır (Alsadı, Yıldırım, Gulsecen, Kose, & Coskun, 2019). Bu kayıtların sonradan yapılabilecek müdahalelere karşı da korumalı olması gerekmektedir. Kaza ile ilgili bilgi ve tutanakların gerek ilgili emniyet trafik şube birimlerince gerekse sigorta kurumları tarafından veri bütünlüğü sağlanacak şekilde saklanması, veri sahteciliği ve tutarsızlıklarına karşı korunması ve gerektiğinde kolayca ulaşılabilir olması da oldukça önemlidir.

İkinci el araç alım-satım süreçlerinde güvenilirliğin sağlanması için araçların geçmişine ait bakım, onarım ve teknik servis kayıtları gibi bilgilere erişim de oldukça önemlidir. Sigorta Bilgi ve Gözetim Merkezi web sayfası ya da kısa mesaj (SMS) ile kayıt altına alınmış hasar kayıtlarına ücretli olarak ulaşılabilmesine rağmen, hileli işlemlerin, kayıt altına alınmayan veya bildirilmeyen kaza, tamir ve parça değişimlerinin, tutulan kayıtların manipüle edilme risklerinin varlığı nedeniyle ikinci el araç pazarında halen güvensizlik hakimdir (Tanrıverdi, Uysal, Üstündağ, & Ayaz, 2021).

Özet olarak araçlarla ilgili veri kayıt çeşitliliğini şu başlıklar altında listeleyebiliriz;

- **Araç Kimlik ve Tanımlama Bilgileri:** Araç kimlik numarası, (Vehicle Identification Number, VIN), araç plakası, şasi numarası, motor numarası, marka, model, üretim yılı gibi temel ve teknik bilgiler.
- **Sahiplik ve Mülkiyet Bilgileri:** Araç sahibi, önceki sahipler, mülkiyet transfer tarihleri ve tescil kayıt belge ve bilgileri.
- **Bakım ve Onarım Kayıtları:** Periyodik bakım geçerlilik tarihleri, yapılan onarımlar, değiştirilen parçalar ve servis raporları.
- **Yakıt ve Emisyon Verileri:** Yakıt tüketimi, emisyon test sonuçları, egzoz gazı ölçümleri ve çevresel performans kayıtları ile elektrik araçlara ait batarya performans ve değişim bilgileri.
- **Sigorta Kayıtları:** Sigorta şirketi, zorunlu trafik poliçe bilgileri, teminat bilgileri, geçerlilik tarihleri, prim ödemeleri ve hasar talep ve takip bilgileri.
- **Kaza ve Hasar Kayıtları:** Kaza geçmişi, hasar tespit raporları, tamir masrafları ve hasar değerlendirmeleri.
- **Kullanım ve Performans Verileri:** Araç kilometresi, hız, yakıt verimliliği, sürüş alışkanlıkları ve araç performans verileri.
- **Yasal ve Düzenleyici Bilgiler:** Trafik ihlal cezaları, muayene tarihleri ve geçerliliği, yasal belgeler ve düzenleyici uyumluluk bilgileri.

Bu veri kayıtları, araçların güvenliğini, performansını ve yasal uyumluluğunu sağlamak için kritik öneme sahiptir. Ayrıca, araçların bakımını ve yönetimini daha etkili hale getirir.

3. Materyal ve Yöntemler

Bu bölümde araçlarla ilgili birçok verinin ortak bir platform üzerinde saklanmasında ve yönetilmesinde etkili ve önemli araç ve teknolojilerin temel özellikleri tanıtılmaktadır.

3.1. Blokzincir Teknolojisi

Blokzincir ilk önce Bitcoin kripto para işlemlerinin, üçüncü bir tarafa güvenmek zorunda kalmadan değiştirilemez kayıtlarını tutmak, işlem sahiplerinin gizliliğini ve veri bütünlüğünü korumak, şeffaf ve denetlenebilir dağıtık bir ağ ortamında depolamak için tasarlanmış ve kullanılmıştır. Bitcoin başta olmak üzere diğer kripto paraların altyapısını oluşturan blokzincir teknolojisinin temel ilkeleri ilk olarak Satoshi Nakamoto'nun 2008 tarihli "Eşler Arası Elektronik Bir Ödeme Sistemi, Bitcoin " (Nakamoto, 2008) başlıklı makalesinde ortaya konmuştur. Blokzincir halka açık, genel kullanımlı ve paylaşımlı bir defter olarak kabul edilebilir ve geçerliliği onaylanmış tüm işlemler zaman damgalı ve birbiri ardına dizilmiş bloklar dizisi olarak saklanır, yeni bloklar eklendikçe büyür. Kullanıcı güvenliği ve defter tutarlılığı için asimetrik kriptografi ve dağıtık mutabakat algoritmaları kullanılmıştır (Zheng, Xie, Dai, Chen, & Wang, 2017).

Blokzincir teknolojisinin yapısal özellikleri olan kriptografik güvenlik, merkeziyetsizlik, şeffaflık, denetlenebilirlik ve mutabakata dayalı, akıllı sözleşmelerle yürütülen işlem onay süreçleri gibi özellikleriyle birçok sektörde iş akış yöntemlerinin iyileştirilmesi ve değiştirilmesinde önemli bir etki oluşturması beklenmektedir. Bu nedenle sayıları giderek artan finans, sağlık ve emlaktan, kamu yönetimi, enerji ve ulaşıma kadar çeşitli sektörlerde kullanılabilecek uygulamalar ve çalışmalar yapılmaktadır (Mendi, 2021).

Blokzinciri teknolojisi yapısal olarak izinli ve izinsiz olarak iki türde kullanılmaktadır. İzinsiz blokzincirleri herkesin anonim olarak ağa katılmasına ve herhangi bir kısıtlama olmaksızın işlem doğrulama süreçlerine katılmasına izin verir. Bu türün önde gelen örnekleri arasında Bitcoin ve Ethereum'un yanı sıra çeşitli diğer kripto para birimleri ve merkezi olmayan ve açık bir yapı sergileyen blokzincir ağ uygulamaları yer alır. İzinsiz blokzincirlerde katılımcılara güven olmadığı için iş kanıtına (Proof of Work, POW) ya da hisse kanıtına (Proof of Stake, POS) dayanan veya Bizans hatalarına (Byzantine Fault Tolerance, BFT) dayanıklı mutabakat mekanizmalarıyla ağ sistemine güveni sağlarken izinli blokzincir ağlarında seçilmiş bir grup düğümün mutabakat (Raft, Kafka vb.) ve işlem doğrulaması sağlaması yeterli görülmektedir (Vukolic, 2016). İzinli blokzincirleri katılımcıların kimliklerinin bilinmesini gerektirir ve genellikle üyelik ve erişim için diğer katılımcıların onayının alınmasını zorunlu

kılar. Ayrıca, bazı izinli blokzincirleri ağ içindeki üyelerin yetki düzeylerini ve rollerini tanımlayarak güvenlik ve uyumluluğu artıran daha kontrollü bir ortam oluşturur.

Blokzincir, kripto para ve finans işlemlerinin ötesinde birçok gizlilik ve güvenliğin önemsendiği sistemlerde de başarıyla uygulanmıştır. Blokzincir teknolojisinin, birçok sektör için iş akış ve veri yönetim modellerinde önemli değişimler oluşturabilecek potansiyelde olduğunu düşündüren, değişmezlik, şeffaflık ve izlenebilirlik gibi temel özelliklerinin yanında doğrulama ve onaylamanın güvenilir üçüncü taraflara ihtiyaç duyulmadan yapılabildiği, güvenliği ve güvenilirliği ile öne çıkan bir yöntem sağlamasıdır. Ancak sağladığı faydalar yanında ölçeklenebilirlik, işlemlerin gecikme süreleri, zaman alan mutabakat süreçleri, blok başına sınırlı veri depolama ve işlem kapasiteleri noktasında hala bazı eksiklikleri bulunmaktadır. Blokzincirde özellikle ölçeklenebilirlik büyük bir endişe kaynağıdır. Örneğin, Bitcoin blok boyutunun 1 MB ile sınırlı olması ve yaklaşık her on dakikada bir blok çıkarılabilmesi, dolayısıyla saniyede en fazla 7 işlem hız sınırına sahip olması, yoğun işlem yükü gerektiren uygulamalar karşısında önemli bir sorun oluşturmaktadır (Zheng et al., 2017).

Blokzincir işlemlerin kaydedilmesinde sipariş-yürütme modelini kullanır. İşlemler sırayla gerçekleştirildiğinden işlem boyut ve sayısının artması bazı darboğaz sorunlarına neden olabilmektedir. Bu durum verimin düşmesi ve gecikmenin artmasına neden olabilmektedir. Bu nedenle blokzincirin büyük boyutlu verilerin depolanmasında kullanılması önerilmez. Büyük boyutlu veriler için blokzincirin dışında zincir dışı olarak tanımlanan özellikle IPFS gibi harici veri ve dosya depolama yöntemleri tercih edilebilir (Ali et al., 2022).

3.2. Hyperledger Fabric ve Temel Özellikleri

Hyperledger Fabric 2015 yılında Linux Foundation tarafından tanıtılmış ve özellikle kurumsal iş uygulamalarında kullanılmak üzere geliştirilmiş, açık kaynak kodlu, modüler ve ölçeklenebilir özellikleri ile öne çıkan gizlilik ve mahremiyet sağlayan izinli bir blokzincir platformudur. Hyperledger Fabric özelleştirilebilir ve izinli yapısıyla birlikte modüler ve değiştirilebilir mutabakat mekanizması, kimlik sertifika sistemi, güncellenebilir dağıtılmış akıllı sözleşmeleri, özel veri iletişimi ve izinli erişim kontrolü sağlayan özellikleriyle kurumsal uygulamalar için daha çok tercih edilmektedir (HLF Docs, 2024). Birçok blokzincir platformunda kullanılan, işlemlerin deftere kaydedilmesi için sipariş-yürütme modeli Hyperledger Fabric'te farklı olarak yürütme-sipariş-doğrulama modeli şeklinde uygulanır. İzinli Hyperledger Fabric platformunda katılımcılar onay ve yetkileri varsa defterde saklanan bilgilere erişebilmektedir. Hangi katılımcıların onay ve erişim yetkisinde olduğu ağın kurulumunda tanımlanan onay politikaları, kanal üyelik ve konfigürasyon yapılandırmaları ile belirlenir.

3.2.1. Hyperledger Fabric Temel Bileşenleri

Organizasyonlar ve Eş Düğümler (Orgs, Peers): Hyperledger Fabric temel yapı taşlarından olan Organizasyonlar ağın yönetimi, veri kontrolü ve politika belirleme gibi görevleri gerçekleştirirler. Her organizasyon kendilerine ait düğümlerin ve kullanıcılarının kimlik ve sertifika yönetimini ve yetkilerini belirler. Bir veya birden fazla kanal üzerinden farklı organizasyonlarla iş birliği yaparak, belirlenen kanal yapılandırma ve onay politikalarına göre işlemlerin onay süreçlerine katılabilirler. Her organizasyon kendi eş düğümlerini yönetir ve eş düğümler üzerinde özel verilerle birlikte kayıt defterlerinin bir kopyasının tutulmasını sağlar. Eş düğümler ise onaylanmış işlem verilerinin kayıt defterinde ve durum veritabanında tutulmasını ve verilerin güvenliği ve erişilebilirliğini sağlar. Eş düğümler iş kurallarına göre akıllı sözleşme zincir kodunu (chaincode) çalıştırarak işlemlerin onay süreçlerini gerçekleştirir. Diğer eş düğümlerle özel bir protokol üzerinden (Gossip) iletişim kurarak işlem tekliflerinin ağda yayılımını ve kayıt defterlerinin tutarlılığını sağlar. Blokzincir ağında eş düğümlere farklı roller tanımlanabilmektedir. Onaylayıcı eş düğüm (Endorsing Peer) istemciden gönderilen işlem tekliflerini akıllı sözleşme kodlarını yürüterek doğrulmasını yapan ve onay veren düğümlerdir. Taahhüt eden eş düğüm (Comitting Peer) işlem onay sürecine katılmaz, oluşturulan bloklardaki işlemleri doğrulayıp kendi kayıt defterlerine ekler. Çapa eş düğüm (Anchor Peer) diğer organizasyonların eş düğümleri ile iletişimi sağlar. Organizasyon içinden seçilen bir lider düğüm (Leader Peer) işlemlerin koordine edilmesi ve diğer eş düğümlere dağıtılması görevini üstlenir.

Sipariş Düğümü (Orderer): Ağda bulunan bir veya birden fazla Orderer düğümü ağdaki farklı eş düğümlerden gelen onaylanmış işlemleri zaman damgaları ve diğer bazı kriterlerine bakarak belirli bir sıraya göre düzenler. Sıralanmış işlemler bloklar halinde gruplandırılır. Daha sonra kayıt defterindeki en son bloğa kriptografik olarak bağlanır ve blokzinciri oluşturulur ve ağda dağıtır. Birden fazla Orderer düğümü varsa ağdaki tüm Orderer düğümlerinin işlemlerin sıralanması ve blok oluşturulmasında karara varabilmeleri için konsensüs mekanizması kullanılır. Hyperledger Fabric, Solo, Kafka, Raft ve Smart BFT konsensüs algoritmalarının kullanımını desteklemektedir.

Kanal (Channel): Hyperledger Fabric'te bulunan çok kanallı ağ yapılandırması kurumsal blokzincir uygulamaları için güçlü ve esnek bir temel oluşturmayı sağlamaktadır. Ağdaki tüm katılımcılar bir veya birden fazla kanala üye olarak birbirleriyle özel ve güvenli iletişim kurabilirler. Her kanalın üyeleri, özellik ve yapılandırmaları farklı olabilir. Katılımcılar birden fazla kanalda rol alabilirler ve böylece farklı iş süreçleri için özel uygulamalar geliştirme imkânı ve ölçeklenebilirlik sağlanır. Her kanalın kendine özel yapılandırılmış ayrı kayıt defteri (Ledger) vardır ve sadece kanal üyeleri tarafından bu deftere erişilebilir. Böylece hassas ve özel veriler aynı kanalda yer almayan diğer üyelere karşı gizlenebilir. Kanal üzerinde yapılacak işlemlerde her üyenin yetkileri ayrı ayrı tanımlandığı gibi kanalda tanımlı Üyelik Hizmet Sağlayıcı (Membership Service Provider, MSP) ile üyelerin ve kullanıcıların sertifika geçerliliği ve kimlik doğrulamaları yapılarak sadece yetkili kullanıcıların deftere erişmesi ve işlem yapması sağlanır. Kanala göre değişen farklı akıllı sözleşmeler (zincir kodları) üzerinden iş süreçleri ve kuralları tanımlanabilir ve güncellemeler yapılabilir.

- **İşlem (Transaction) Veri Yapısı:** Araçlar için kayıt altına alınabilecek bilgi çeşitliliği oldukça fazladır. Önerilen model aracın kimlik bilgisiyle bağlantılı sınıflandırılmış verilerin kaydını sağlamak için bir altyapı oluşturmaktadır. Bu bağlamda araca ait bilgiler anahtar-değer (key-value) çifti şeklinde iki alan tanımlanarak kayıt altına alınır ve sorgulamalar anahtar alanında kullanılan araç kimliğiyle yapılır. Değer alanı içerisinde kaydın sınıf tanımı ile birlikte diğer bilgiler JSON veri yapısında veya dizi şeklinde yapılandırılmaktadır.
- **Kayıt Yeri:** Önerilen modelde kullanılan Hyperledger Fabric blokzincir platformunda işlemler hem durum veritabanında hem de kayıt defteri içinde birbiriyle kriptografik olarak bağlantılı bloklar içerisinde anahtar-değer çifti şeklinde organize edilerek kayıt altına alınmaktadır. Hyperledger Fabric durum veritabanı olarak LevelDB ya da CouchDB'nin kullanımını desteklemektedir. Durum veri tabanları hızlı ve verimli sorgulama ve okuma yapabilmek için optimize edilmiştir ve kriptografik yöntemlerle güvence altına alınmıştır. Kayıt defteri ise tüm işlem geçmişini değiştirilemez, kurcalamaya karşı korumalı, kriptografik olarak birbirine bağlı blokzincirleri içerisinde tutmaktadır.

Sertifika Otoritesi (Certificate Authority, CA) ve Üyelik Hizmet Sağlayıcı (MSP): Hyperledger Fabric mimarisinde her kuruluş, düğüm ve son kullanıcıların dijital sertifika (x.509) veya kimlik doğrulama (Identity Mixer, Idemix) teknolojileri ile sağlanan sertifikalar ile dijital bir kimliğe sahip olması gerekmektedir. Fabric ağında kullanıcıların ve düğümlerin yetkileri ve özellikleri sertifikalar aracılığıyla tanımlanmaktadır. Bu nedenle sertifikaların güvenilir olması ve güvenilir bir kaynaktan üretilmeleri oldukça önemlidir. Hyperledger Fabric mimarisinde sertifikaların üretilmesi ve dağıtılması için Fabric CA sertifika yetkilisi kullanılabileceği gibi başka sertifika üretimi sağlayan (Openssl, Trusted CA vb.) araçlarda tercih edilebilmektedir. Hyperledger Fabric mimarisinde Açık Anahtar Altyapısı (Public Key Infrastructure, PKI) yöntemleri ile dijital sertifikaların üretilmesi, dağıtılması, kullanılması, yenilenmesi, iptal edilmesi ve doğrulanması gibi süreçlerin yönetimi için her kuruluş için MSP modülü kullanılmaktadır. Hyperledger Fabric'te sertifika yönetimi ve açık anahtar altyapısının merkezi olması, katılımcı düğüm sayısı çok arttığında ve kullanıcılar aynı anda büyük hacimli işlemler gerçekleştirmeye çalıştığında bir darboğaz oluşabilmekte verim düşüklüğü ve ölçeklenebilirliğin azalması söz konusu olabilmektedir (Abubakar, McCarron, Jaroucheh, Al Dubai, & Buchanan, 2021).

Akıllı Sözleşmeler (Smart Contract): Blokzincir ağında dağıtık kayıt defterine kaydedilecek işlemlerin oluşturulması için, tanımlanan koşullara göre tetiklenen, taraflar arasındaki sözleşme koşullarına göre merkezi bir otoriteye ihtiyaç olmadan işlemleri otomatik olarak yürütebilen, geri dönük değişimin mümkün olmadığı bilgisayar programlarıdır. Blokzincir ağ uygulamasına gömülü olan Akıllı

Sözleşme kodları ağdaki tüm düğümler tarafından dağıtık defter kaydı ve işlem verileri ile birlikte depolanmakta ve düğümlerdeki sunucular üzerinde çalıştırılmaktadır.

Hyperledger Fabric'te akıllı sözleşmeler, zincir kodu (chaincode) olarak bilinir. Zincir kodu tanımlanan bir kanal üzerinde, onay politikalarına göre yetkilendirilmiş kuruluşların eş düğümlerine kurulur ve senkronize edilir. Gerektiğinde yetkili bir kuruluş tarafından zincir kodu güncellenebilir. Zincir kodunda yer alan algoritma belirlenen iş mantığının doğru yürütülmesi için bir güvence sağlar. Hyperledger Fabric'te Zincir Kodları Java, Golang, TypeScript ve Javascript programlama dilleri ile programlanabilmektedir.

3.3. Dağıtık Dosya Depolama Sistemi (Interplanetary File System, IPFS)

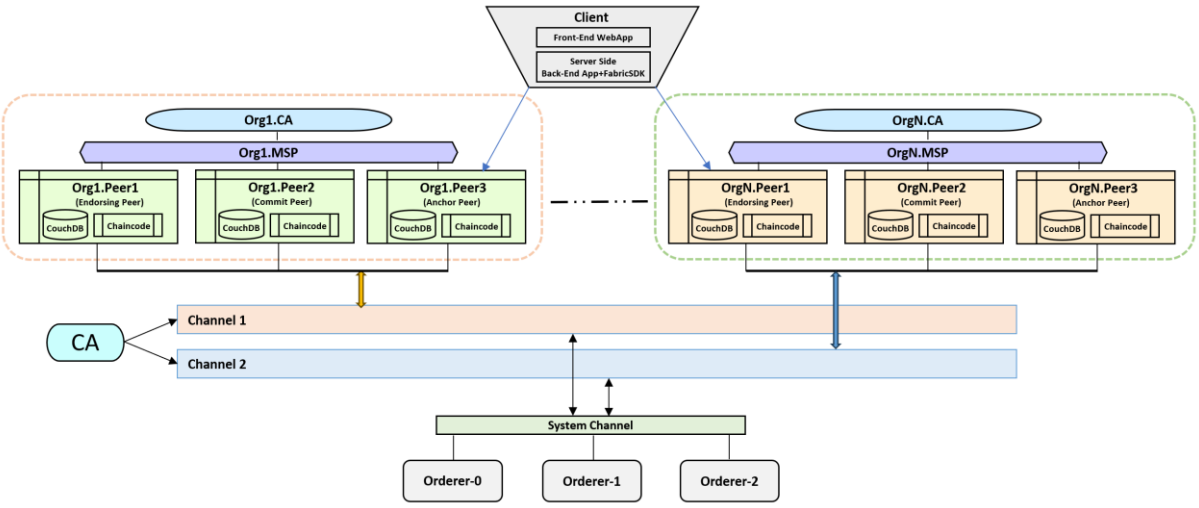
IPFS, merkezi olmayan, dağıtık, eşler arası bir dosya depolama protokolüdür, İlk sürümü 2015 yılında yayınlanmış ve açık kaynak kodlu dağıtık bir dosya depolama sistemi olarak kullanıma sunulmuştur. Blokzincir ve DLT uygulamalarında zincir dışı veri ve dosya depolama ortamı olarak tercih edilebilir. Merkezi sistemlerin tek hata noktası gibi sorunlarını çözen, bütünlüğün korunmasında etkili bir yöntem sunan IPFS, mevcut web sisteminin dağıtık web'e dönüşmesini ve sansüre dayanıklı web sitelerinin oluşmasına katkı sağlaması beklenmektedir. İnternet ortamında genel bir kullanıma sahip olduğu gibi, izole edilmiş özel bir ağda dosya paylaşım sistemi olarak da kullanılabilmektedir. IPFS'in herkese açık ağ yapısına sahip olması nedeniyle, depolanacak dosyaların önceden şifrelenmesi verilerin ifşasını korumak ve gizlemek için gereklidir. Aksi halde dosya erişim bilgisine sahip herkes tarafından dosyalara erişilebilir. IPFS'in kurumsal kullanımları için özelleştirilmesi ve sadece izin verilen düğümler arasında veri paylaşımının yapılması gizliğin de korunmasına katkı sağlayacaktır (Abdullah Lajam & Ahmed Helmy, 2021; Ali et al., 2022).

4. Önerilen Modelin Temel Bileşenleri ve Özellikleri

4.1. Hyperledger Fabric Blokzincir Platformu

Hyperledger Fabric, kurumsal uygulamalar için güçlü bir blokzincir platformudur. Gizlilik, ölçeklenebilirlik, esneklik, güvenlik ve entegrasyon gibi avantajları sayesinde, birçok farklı sektörde ve farklı ihtiyaçlardaki kurumsal uygulamalar için uygun bir çözüm sunar.

Önerilen modelde araçlarla ilgili işlem kayıtlarının tutulması ve veri yönetiminde altyapı oluşturmak için Hyperledger Fabric blokzincir platformu kullanılmıştır. Araçlarla ilgili işlemlerde rol alan birçok kuruluş ve çok sayıda kullanıcı vardır. Çok sayıda katılımcının olduğu ortak bir platformda iş birliğini sağlamak ve işlemlerin güvenli ve güvenilir bir kaydını tutabilmek için gelişmiş bir kimlik doğrulama ve denetlenebilir ve izlenebilir bir veri yönetimine ihtiyaç vardır. Hyperledger Fabric platformunun yapısal özellikleri bu ihtiyaçları karşılayabilecek potansiyeldedir. Şekil 2'de gösterildiği gibi, çoklu organizasyon ve her organizasyonun kontrolünde çok sayıda katılımcının yer aldığı, iki kanallı bir Hyperledger Fabric blokzincir ağ mimarisi tasarlanmıştır. İki kanallı blokzincir ağında kanal 1, ağdaki kullanıcıların üyelik ve kimlik bilgilerinin saklandığı kayıt defterinin yönetimini, kanal 2 ise araçlarla ilgili işlem kayıtlarının tutulduğu kayıt defterinin yönetimini sağlamak için kullanılmaktadır.



Şekil 2. Önerilen blokzincir mimarisi

İstemci Yazılımı (Client-WebApp): İstemci yazılımı, web arayüzü (front-end) ve sunucu yazılımı (back-end) olmak üzere iki kısımdan oluşmaktadır. Web arayüzü, kullanıcı ile etkileşim kurmak, sunucu yazılımına bilgi girişi ve sorgu göndermek için mobil telefon ya da bilgisayar üzerinde çalışan javascript tabanlı uygulamadır. Sunucu yazılımı ise Hyperledger Fabric ağına bağlanmak ağdaki eş düğüm ve akıllı sözleşme zincir kodlarıyla etkileşim kurmak için Fabric SDK ve API'lerini kullanan Node.js, Java ya da Go programlama dillerinde yazılmış bir uygulamadır. Hyperledger Fabric istemci yazılımları, güvenli ve izinli bir ağda çalıştığı için tüm işlemler ve etkileşimler sertifikalarla doğrulanır ve dijital imza yöntemleriyle güvence altına alınır.

İstemci yazılımı, her organizasyonun görev ve sorumluluklarına göre özel olarak tasarlanır. Blokzincir kayıt defterinde kayıt altına alınmak istenen İşlemlere ait bilgiler anahtar-değer çifti oluşturacak şekilde ve JSON veri yapısında düzenlenmelidir. Kanal-1 üzerindeki kayıt defteri ağdaki kullanıcıların yönetimi için kullanılmaktadır. Kullanıcılara ait hesap bilgileri kaydedilmek istendiğinde Anahtar alanı kullanıcı kimliği olmalı ve değer alanı ise kullanıcının detay bilgilerini içermelidir. Kanal-2 üzerindeki kayıt defteri ise araçlara ait verilerin yönetimi için kullanılmaktadır. Araçlarla ilgili gerçekleştirilen işlem bilgileri kaydedilmek istendiğinde Anahtar alanı araç kimliği (VIN) olmalı ve değer alanı ise gerçekleştirilen işleme ait detay bilgilerini içermelidir.

Kullanıcı ve Sertifika Yönetimi: Araçlara ait işlemler için bilgi giriş ve sorgulamaları çeşitli yetki ve sorumluluklara sahip kullanıcılar tarafından yapılmaktadır. Her organizasyon kendi sorumluluk alanındaki işlemleri yapması için öncelikle kullanıcılarını tanımlayan yetki ve rollerini belirleyen kaydı kanal-1'deki kayıt defterine girmelidir. Ağ üzerinde işlemlerin yapılması için dijital sertifika ve dijital imzalar kullanılmaktadır. Her organizasyonun sahip olduğu sertifika yöneticisi (Org1.CA) kendi eş düğüm ve kullanıcılarına geçerliliği kontrol edilebilen bir sertifika sağlamakla görevlidir. Bu sertifika ve dijital imzalar ağ içerisinde, iletişimin güvenliğini sağlama ve işlemlerin doğrulanmasında kullanılmakta, Organizasyona ait Üyelik Servis Sağlayıcı (Org1.MSP) tarafından sertifika ve dijital imzaların geçerliliği kontrol edilmektedir. Önerilen modelde, araç sahipleri, özel/resmî kurumların yetkili personelleri, sigorta acente çalışanları, oto servis ve tamir-bakım yetkilileri ve araçlara ait veri aktarımı yapan IoT cihazları kullanıcı olarak tanımlanır ve atanan yetki, rolleri ve sertifikaları ile Kanal-1'e ait kayıt defterine kaydedilir.

Organizasyon ve Eş Düğümler: Hyperledger Fabric, kullanımda olan ağa yeni organizasyon ve eş düğümlerin eklenmesine imkân veren esnek bir yapıdadır. Bu özellik, önerilen model için araçlarla ilgili yeni işlemlerin kaydını yapabilmeyi, çeşitli hizmetler için veri yönetimini sağlamayı mümkün hale getirecektir. Ağa yeni organizasyonların eklenebiliyor olması ağın, merkeziyetsiz özelliğini daha da geliştireceği gibi, yük dengeleme, tek nokta hatalarına karşı daha dirençli hale gelme, yedekliliğin artması ve iş birliği potansiyelini artırmaya yönelik birçok fayda sağlayacaktır. Şekil 2'de önerilen

mimari yapı birçok organizasyon çok kanallı bir platform üzerinde birlikte çalışabilirliğini göstermektedir. Eş düğümler (peers) organizasyona göre değişen sayılarda tanımlanabilir, sonradan ekleme de yapılabilir. Eş düğümler üyesi olunan kanala ait kayıt defterlerinin bir kopyasını tutmaktadır. Kanal onay politikalarına, akıllı sözleşme kod kurallarına ve yapılandırmaya göre kayıt defterine yazılması için işlem teklifi ve sorgulama için durum veri tabanına (CouchDB veya LevelDB) erişim sağlayabilirler. Her eş düğüm, ağda yayımlanan ve yeni oluşturulan blokların işlem ve geçerlilik doğrulamalarını yaparak kendi kayıt defterlerindeki blokzincirini günceller.

Önerilen modelde organizasyonlar ve görevleri:

- **Org1 (Emniyet Genel Müdürlüğü Trafik Başkanlığı):** Araç tescil işlemleri, plaka işlemleri, kaza takip işlemleri, trafik denetim, ihlal ve ceza işlemleri, yasal takip ve sorgulamalar. İl ve ilçelere, işlem yük dağılımına göre çok sayıda eş düğüm tanımlama ve yönetme. Araç sahibi ve yetkili personel için kullanıcı kayıt ve yönetimi.
- **Org2 (Noterler Birliği):** Trafik tescil işlemleri, araç alım-satım tescil işlemleri. Eş düğüm yönetimi. Araç sahibi ve yetkili kullanıcı kayıt ve yönetimi.
- **Org3 (Sigorta Şirketleri):** Zorunlu trafik sigortası, araç kaza ve hasar yönetimi. Yetkili acente personeli kullanıcı yönetimi.
- **Org4 (Araç Muayene Şirketleri):** Araç muayene işlemleri, egzoz emisyon ölçüm işlemleri. Yetkili personel kullanıcı yönetimi.
- **Org5 (Oto Servis ve Tamirhaneler):** Araç tamir, bakım ve yedek parça değişim işlemleri. Özel servis yetkilileri, onarım ve bakım için kayıt girme yetkisi almış tamirhane personeli kullanıcı yönetimi.
- **Org6 (Diğer Kurumlar):** Diğer ihtiyaç duyulan hizmetler için tutulacak kayıtlar. HGS/OGS otomatik geçiş takip, Araç içi veri takibi için IoT cihaz yönetimi vb.

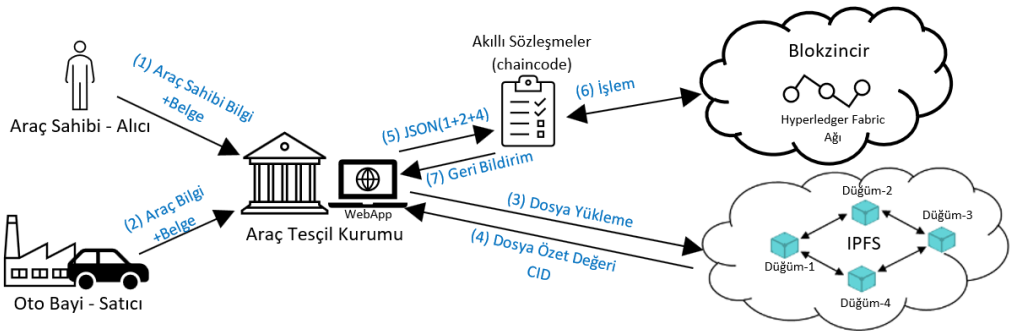
4.2. Özel Dağıtık Dosya Depolama (Private IPFS)

IPFS, kurumsal uygulamalarda veri dayanıklılığı, güvenlik, maliyet tasarrufu, performans, şeffaflık ve merkeziyetsizlik gibi birçok avantaj sunar. Bu avantajlar, IPFS'i özellikle büyük veri setleri, hassas bilgiler ve merkezi olmayan uygulamalarla çalışan kurumlar için cazip bir seçenek haline getirir (Majdak, 2023).

Önerilen modelde IPFS teknolojisinin kullanılmasının amacı, araçlarla ilgili gerçekleştirilen işlemlerde gerekli olan ek bilgi ya da kanıt hükmündeki belge, fotoğraf, ses ve görüntü gibi her türlü dosya türünün dağıtık bir ağda saklanarak erişilebilirliğini ve bütünlüğünü korumak ve çoklu yedeklilik sağlamaktır. Böylece dosyaların birden fazla kopyası dağıtık bir ağda tutulduğu için veri kayıp riski azaltılmış, tek nokta hatasından kaynaklanabilecek problemler ortadan kaldırılmış, her daim hızlı bir şekilde erişilebilirlik sağlanmış olacaktır.

Önerilen Modelde Özel IPFS Ağının Kullanımı:

Kullanıcılar, işlemlere ait bilgileri web arayüzü üzerinden blokzincir ağına göndermeden önce işlemlerle ilgili çeşitli türdeki dijital belge ve dosyaları özel IPFS ağına yükler. IPFS ağına yüklenen her dosyanın hash değeri ile oluşturulmuş olan CID bilgisi işlem verilerine dahil edilerek blokzincir ağına, araç kimlik bilgisi ile birlikte JSON veri yapısında gönderilir. Daha sonra yapılacak sorgulamalarda CID bilgisi IPFS ağında dosyaya erişmek için kullanılır. Özel IPFS ağına gönderilen dosyalar ağda bulunan tüm düğümlere dağıtılmaktadır. Özel IPFS ağındaki dosyalara genel IPFS ağından erişim sağlanamadığı gibi özel ekip anahtarı (swarmkey) olmayan düğümlerle iletişim de kurulamadığı için gizlilik ve güvenlik korunmuş olur.



Şekil 3. Araç tescil kaydına ait bilgi ve belgelerin yüklenmesinde işlem akış sıralaması

IPFS ağına dosya yükleme süreci, araç tescil kaydı işlemi üzerinde örneklenerek Şekil 3'de gösterilmektedir. Araç alım-satım süreciyle ilgili araç tescil kaydına ait işlemlerde; (1) alıcı ve (2) satıcı kimlik bilgileriyle birlikte araca ait istenen bilgi ve belgelerle araç tescil kurumuna başvurur. Araç tescil kuruluşundaki yetkili personel blokzincir ve IPFS ağıyla etkileşim kurmak için gerekli sertifika ve dijital imzalara sahiptir. Yetkili personel, kurumun WebApp kullanıcı arayüzü üzerinden tescil kaydı için gerekli bilgileri girer. Kâğıt tabanlı belgeler dijital dosyaya dönüştürülerek (3) IPFS ağına yüklenir. IPFS ağına yüklenen her dosya için (4) dosyaya ait hash değeri (CID) WebApp arayüzüne döndürülür. WebApp arayüzü üzerinde (5) toplanan bilgiler Blokzincir ağında ilgili akıllı sözleşme zincir koduna gönderilir. Akıllı sözleşme zincir kodu işlemleri yürüterek doğrular, (6) kayıt defterine yazılması için blokzincire gönderir ve (7) yürütülen işlem sonucunu WebApp' ye bildirir.

IPFS ağına yüklenen dijital belge ve dosyaların hash değerleri işlem kaydı içerisinde akıllı sözleşme koduna gönderilmiş ve doğrulanan işlemlerle birlikte kayıt defterinde saklanmıştır. Daha sonra işlem kaydı sorgulandığında hash değeri ile IPFS ağındaki ilgili dosyaya erişim sağlanabilecektir. Dosyalara ait hash değerinin bilinmesi dosyanın içeriğine ulaşmak için yeterli olduğundan hassas veriler içeren dosyalar için gizlilik problem olacaktır. Gizliliğin sağlanması için dosyaların IPFS ağına yüklenmeden önce şifrelenmesi ve şifre anahtarının da korunması için ayrı bir mekanizmanın oluşturulmasına ihtiyaç vardır.

5. Sonuç

Yapılan çalışmada araçlarla ilgili kayıt altına alınan bilgi çeşitliliği ve veri yönetimi için literatürdeki çalışmalar ve geliştirilen uygulamalar için kullanılan yöntem ve teknolojiler incelenmiştir. Bu çalışmada önerilen araçların blokzincir tabanlı veri yönetim modeli, aracın yaşam döngüsü içerisinde gerçekleştirilen birçok işlemde rol alan resmi ve özel birçok kurumun, şeffaf, güvenli ve güvenilir bir platform üzerinde iş birliği yaparak veri takibi ve yönetimini yapabilmesini hedefleyen kapsamlı bir yaklaşım sunmaktadır.

Modelin temel amacı, aracın tarihçesini oluşturmak için, araçla ilgili gerçekleştirilen işlemlere ait kayıtların, aracın ilk tescil kaydında belirlenen benzersiz araç kimlik numarası ile ilişkilendirilerek zaman damgalı ve değiştirilemez bir şekilde, dağıtık bir ağda depolanmasını sağlamaktır. Bu sayede araçların birçok işlem için izlenebilirliğini ve denetlenebilirliğini kolaylaştırarak sahte ve hileli işlemlerin, dolandırıcılık ve hırsızlık gibi sorunların engellenmesine, veri eksikliği ve kanıt ve belge yetersizliğinden kaynaklanan güvensizliklerin ortadan kalkmasına katkı sağlaması hedeflenmektedir.

Önerilen model, ikinci el araç alım-satım işlemleri, çeşitli tescil işlemleri, zorunlu araç sigortası ve muayenesi, araç kaza ve hasar yönetimi, bakım onarım ve yedek parça değişim işlemleri, trafik ihlal ve ceza işlemleri gibi birçok hizmetin takip ve yönetiminde kullanılabildiği gibi, modelin ölçeklenebilir ve genişletilebilir özellikteki altyapısı sayesinde, araç kiralama, filo yönetimi, paylaşımlı hareketlilik, park yönetimi, bağlantılı araçlar, elektrikli yada otonom araçlara ait özel hizmetler ile köprü yada otoyol otomatik geçiş takip ve yönetimi gibi bir çok hizmetin de daha güvenli ve verimli bir şekilde gerçekleştirilmesi mümkün olacaktır. Ancak mevcut potansiyelin tam olarak kullanılabilir olması ve sistemin başarısı için sistemde rol alan kurum ve kuruluşların kullanılan teknolojileri benimsemesi, iş

birliğinin sağlayacağı faydalara güvenmeleri ve veri girişlerinde gerekli hassasiyeti göstermeleri gereklidir.

Sonuç olarak tasarlanan ve önerilen model, Hyperledger Fabric ve IPFS gibi yenilikçi teknolojilerin entegrasyonu ile araçların yaşam döngüsüne ait tüm tarihçesinin ilgili paydaşlar tarafından yetki ve sorumluluklarına göre daha verimli ve güvenli bir şekilde izlemelerine ve yönetmelerine imkân vererek, kurumların mevcut geleneksel iş modelleri üzerinde önemli bir dönüşüm gerçekleştirme potansiyeline sahiptir.

Önerilen modelin araçlara ait işlemleri gerçekleştiren özel ve resmî kurumlar tarafından benimsenmesi ve uygulanması halinde, özellikle ikinci el araç pazarında yaşanan güvensizliklerin giderilmesini, dolandırıcılık faaliyetlerinin azaltılması, sahte ve hileli işlemlerin önüne geçilmesini, araç takip ve denetimlerinin daha kolay yapılabilmesini, kilometre sayacı manipülasyonlarının, sigorta dolandırıcılıklarının engellenmesini sağlayabilir. Ulaşım ve otomotiv sektörünün daha güvenli ve verimli çalışmasına katkı sağlayarak, ulaşım sistemlerinin ve kurumsal süreçlerin dijitalleşmesinde, kâğıt tabanlı belge kullanımın azaltılmasında, maliyetlerin azaltılmasında trafik güvenliğinin artırılmasında önemli katkılar sağlayacağı öngörülmektedir.

Araştırmacıların Katkı Oranı Beyanı

Yazarların çalışmadaki katkı oranları eşittir.

Destek ve Teşekkür Beyanı

Çalışmada herhangi bir destek alınmamıştır. Teşekkür edilecek bir kurum veya kişi bulunmamaktadır.

Çıkar Çatışması Beyanı

Bu makale, Bandırma Onyedi Eylül Üniversitesi, Lisansüstü Eğitim Enstitüsü, Akıllı Ulaşım Sistemleri ve Teknolojisi Ana Bilim Dalı bünyesinde hazırlanan Doktora tezinden üretilmiştir. Çalışma kapsamında herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.

Kaynakça

Abbade, L. R., Ribeiro, F. M., Da Silva, M. H., Morais, A. F. P., Morais, E. S. de, Lopes, E. M., . . . Rodrigues, J. J. P. C. (2020). Blockchain Applied to Vehicular Odometers. *IEEE Network*, *34*(1), 62–68. https://doi.org/10.1109/MNET.001.1900162

Abdullah Lajam, O., & Ahmed Helmy, T. (2021). Performance Evaluation of IPFS in Private Networks. In *2021 4th International Conference on Data Storage and Data Engineering* (pp. 77–84). New York, NY, USA: ACM. https://doi.org/10.1145/3456146.3456159

Abubakar, M., McCarron, P., Jaroucheh, Z., Al Dubai, A., & Buchanan, B. (2021). Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates. In *2021 14th International Conference on Security of Information and Networks (SIN)* (pp. 1–8). IEEE. https://doi.org/10.1109/SIN54109.2021.9699221

Akçi, Y. (2016). İkinci El Omobil: Tüketici Bakışıyla. *Adıyaman Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *1*(1), 329. https://doi.org/10.14520/adyusbd.68749

Ali, H., Ahmad, J., Jaroucheh, Z., Papadopoulos, P., Pitropakis, N., Lo, O., . . . Buchanan, W. J. (2022). Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform. *Entropy (Basel, Switzerland)*, *24*(10). https://doi.org/10.3390/e24101379

Alsadı, M., Yıldırım, S., Gulsecen, S., Kose, B. O., & Coskun, V. (2019). Akıllı Araç Ekosistemlerinde Blockchain Tabanlı Güvenli Veri Yönetim Modeli. In *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies: Ankara, Turkey, October 11-13, 2019* (pp. 1–5). Piscataway, NJ: IEEE. https://doi.org/10.1109/ISMSIT.2019.8932885

ARTES Bilgi Sistemleri (2018). Araç Tescil Sistemi (TescilGerekliEvrak). Retrieved from https://portal.tnb.org.tr/Artes/Sayfalar/TescilGerekliEvrak.aspx

Athanere, S., & Thakur, R. (2022). Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. *Journal of King Saud University, Computer and Information Sciences*, *34*(4), 1523–1534. https://doi.org/10.1016/j.jksuci.2022.01.019

Baumann, J., Zavolokina, L., & Schwabe, G. (2021). *Dealers of Peaches and Lemons: How Can Used Car Dealers Use Trusted Car Data to create value?* HICSS. https://doi.org/10.5167/uzh-192651

Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A., & Ben Hamida, E. (2018). Digitizing, Securing and Sharing Vehicles Life-cycle over a Consortium Blockchain: Lessons Learned. In M. &. S. IFIP International Conference on New Technologies (Ed.), *2018 9th IFIP International Conference on New Technologies, Mobility & Security: Proceedings of NTMS 2018 Conference and Workshop : 26-28 February 2018, Paris, France* (pp. 1–5). Piscataway, NJ: IEEE. https://doi.org/10.1109/NTMS.2018.8328733

Car-Pass (2022). Car-Pass annual report 2022 - News about Car-Pass. Retrieved from https://www.car-pass.be/en/news/car-pass-annual-report-2022

Chanson, M., Bogner, A., Wortmann, F., & Fleisch, E. (2017). Blockchain as a privacy enabler. In *Lee, Takayama et al. (Ed.) 2017 – Proceedings of the 2017 ACM* (pp. 13–16). https://doi.org/10.1145/3123024.3123078

Das, D., Banerjee, S., Ghosh, U., Biswas, U., & Bashir, A. K. (2021). A decentralized vehicle anti-theft system using Blockchain and smart contracts. *Peer-to-Peer Networking and Applications*, *14*(5), 2775–2788. https://doi.org/10.1007/s12083-021-01097-3

Dayı, F., & Hasanoğlu, T. (2023). Türkiye'de İkinci El Otomobil Fiyatlarını Etkileyen Faktörlerin İncelenmesi. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, *14*(38), 436–457. https://doi.org/10.21076/vizyoner.1193474

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

HLF Docs (2024). Hyperledger Fabric. Retrieved from https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html

Holler, M., Barth, L., & Fuchs, R. (2019). Trustworthy Product Lifecycle Management Using Blockchain Technology—Experience from the Automotive Ecosystem. In J. Stark (Ed.), *Decision Engineering. Product lifecycle management. (Volume 4): The case studies / John Stark, editor* (pp. 13–19). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-16134-7_2

Leila Benarous, Benamar Kadri, Ahmed Bouridane, & Elhadj Benkhelifa (2021). Blockchain-based forgery resilient vehicle registration system. *Transactions on Emerging Telecommunications Technologies*. Advance online publication. https://doi.org/10.1002/ett.4237

Majdak, M. (2023). IPFS Private Network. Retrieved from https://startup-house.com/blog/ipfs-private-network-guide

Mendi, A. F. (2021). Blokzincir Uygulamaları ve Gelecek Öngörüleri. *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, *4*(1), 76–88. Retrieved from https://dergipark.org.tr/tr/pub/aist/issue/56936/862936

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

Schwabe, G. (2019). The role of public agencies in blockchain consortia: Learning from the Cardossier. *Information Polity*, *24*(4), 437–451. https://doi.org/10.3233/IP-190147

Tanrıverdi, M., Uysal, M., Üstündağ, M. T., & Ayaz, Z. (2021). Araç Cüzdanı: Motorlu Araçların Teknik Servis ve Bakım Kayıtlarının Blokzinciri Üzerinde Yönetilmesi. *Düzce Üniversitesi Bilim Ve Teknoloji Dergisi*, *9*(4), 1358–1373. https://doi.org/10.29130/dubited.904757

Tektaş, M., Korkmaz, K., & Erdal, H. (2016). Akıllı Ulaşım Sistemlerinin Geleceği (Ekonomik ve Çevresel Faydaları). *Balkan Sosyal Bilimler Dergisi*, 561–577. Retrieved from https://dergipark.org.tr/en/pub/bsbd/issue/43860/539514

Vukolic, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch & D. Kesdoğan (Eds.), *Lecture Notes in Computer Science. Open problems in network security* (Vol. 9591, pp. 112–125). New York NY: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-319-39028-4_9

Zafar, S., Hassan, S. F. U., Mohammad, A., Al-Ahmadi, A. A., & Ullah, N. (2022). Implementation of a Distributed Framework for Permissioned Blockchain-Based Secure Automotive Supply Chain Management. *Sensors (Basel, Switzerland)*, *22*(19). https://doi.org/10.3390/s22197367

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (Eds.) (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.*