ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

HASSAS SAĞLIK VERİLERİNİN BLOKZİNCİR İLE GÜVENLİ ŞEKİLDE TAŞINMASI VE İŞLENMESİ

Eray ÖZCAN

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2025

ÖZET

Yüksek Lisans Tezi

HASSAS SAĞLIK VERİLERİNİN BLOKZİNCİR İLE GÜVENLİ ŞEKİLDE TAŞINMASI VE İŞLENMESİ

Eray ÖZCAN

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Mehmet Serdar GÜZEL

Sağlık sektöründe dijitalleşmenin hızla artmasıyla birlikte, hassas sağlık verilerinin güvenliği, gizliliği, bütünlüğü ve izlenebilirliği kritik bir gereklilik haline gelmiştir. Modern sağlık sistemleri büyük miktarda kişisel veriyi üretmekte ve işlemektedir. Bu veriler, hastaların onayıyla ulusal ve uluslararası otoritelerle paylaşılmakta, ancak bu durum veri güvenliği ve mahremiyet açısından ciddi riskler doğurmaktadır. Siber saldırılar, yetkisiz erişimler ve veri ihlalleri gibi tehditler, kritik sağlık bilgilerinin gizliliğini tehlikeye atmakta; yasal uyumluluk ve geriye dönük doğrulanabilir kayıtların önemini artırmaktadır.

Mevcut merkezi sağlık bilgi sistemleri ise tekil hata noktaları, veri manipülasyonu ve sınırlı şeffaflık gibi sorunlar nedeniyle yetersiz kalmaktadır. Sağlık verilerinin korunması yalnızca gizlilikle sınırlı olmamalı; aynı zamanda güvenli, şeffaf ve değiştirilemez şekilde yönetimi de sağlanmalıdır.

Bu çalışmada, FHIR IPS (International Patient Summary) veri modeline dayalı, blokzincir destekli bir sağlık verisi yönetim çerçevesi önerilmektedir. Blokzincirin dağıtık ve değiştirilemez yapısı sayesinde veriler güvenli biçimde saklanmakta ve işlem geçmişi şeffaf tutulmaktadır. İzinli blokzincir altyapısı ile tasarlanan sistemde veriler kriptografik olarak korunmakta ve ulusal düzenlemelere uyum sağlanmaktadır.

Ayrıca, akıllı sözleşmeler aracılığıyla hasta onam yönetimi, güvenli veri paylaşımı ve erişim kontrolü de sisteme dahil edilmiştir. Böylece paydaşlar arasında güvenli, şeffaf ve hasta odaklı veri paylaşımı mümkün olmakta; veri sahipliği ve birlikte çalışabilirlik ilkeleri korunmaktadır. Bu yaklaşım, sağlık verilerinin bütünlüğünü güçlendirerek modern sağlık sistemlerinde güven ve şeffaflığı artırmaktadır.

Eylül 2025, 53 sayfa

Anahtar Kelimeler: Blokzincir, Veri Güvenliği, Elektronik Sağlık Kayıtları (ESK), Akıllı Sözleşmeler, Dağıtık Defter Teknolojisi, Birlikte Çalışabilirlik, GDPR, İzinli Blokzincir, Müdahaleye Karşı Dayanıklı Sistemler, Sağlık Bilgi Sistemleri, Açık Rıza, HL7, FHIR, Uluslararası Hasta Özeti (IPS)

ABSTRACT

Master Thesis

SECURE TRANSFER AND PROCESSING OF SENSITIVE HEALTHCARE DATA USING BLOCKCHAIN

Eray ÖZCAN

Ankara University
Graduate School of Natural and Applied Science
Department of Computer Engineering

Supervisor: Prof. Dr. Mehmet Serdar GÜZEL

With the rapid digitalization of the healthcare sector, ensuring the security, privacy, integrity, and traceability of sensitive health data has become a critical requirement. Modern healthcare systems generate and process vast amounts of personal data. These data are shared with national and international authorities under patient consent, yet this also creates significant risks regarding data security and confidentiality. Threats such as cyberattacks, unauthorized access, and data breaches endanger the privacy of critical health information, highlighting the need for legal compliance and verifiable records.

However, existing centralized health information systems remain insufficient due to single points of failure, vulnerability to manipulation, and limited transparency. Protecting health data should not only focus on confidentiality but also ensure secure, transparent, and immutable management.

This study proposes a blockchain-based healthcare data management framework built on the FHIR IPS (International Patient Summary) data model. By leveraging blockchain's distributed and immutable structure, data can be securely stored while maintaining a transparent transaction history. Through a permissioned blockchain infrastructure, sensitive health data are cryptographically protected and managed under policy-based ledgers, ensuring compliance with national data protection regulations.

Moreover, smart contracts enable patient consent management, secure data sharing, and access control. This ensures safe, transparent, and patient-centered data exchange among healthcare stakeholders while maintaining principles of data ownership and interoperability. Such an approach enhances resilience against unauthorized modifications and strengthens trust, transparency, and integrity in modern healthcare systems.

September 2025, 53 pages

Keywords: Blockchain, Data Security, Electronic Health Records (EHR), Smart Contracts, Distributed Ledger Technology, Interoperability, GDPR, Permissioned Blockchain, Tamper-resistant Systems, Healthcare Information Systems, Explicit Consent, HL7, FHIR, International Patient Summary (IPS)

ÖNSÖZ ve TEŞEKKÜR

Bu tez çalışması hem akademik merakım hem de mesleki tecrübem doğrultusunda, sağlık verilerinin güvenli yönetimi ve blokzincir tabanlı teknolojiler alanında uzmanlaşma hedefiyle yürütülmüştür. Uzun yıllardır bilgi teknolojileri sektörünün farklı alanlarında edindiğim deneyimler, çalışmanın konu seçiminde yol gösterici olmuştur.

Sağlık sektöründe yaşanan hızlı dijitalleşme, veri paylaşımı ihtiyacının artması ve kişisel verilerin korunmasına yönelik yükselen farkındalık, bu çalışmayı daha anlamlı ve güncel bir zemine taşımıştır. Özellikle uluslararası standartlara uygun, güvenli ve izlenebilir sağlık verisi paylaşımı ihtiyacı, blokzincir teknolojisinin sunduğu yenilikçi çözümlerle birleşerek bu tezin temel motivasyonunu oluşturmuştur. Böylece, tez yalnızca akademik bir araştırma olmanın ötesinde, sektörde karşılaşılan gerçek problemlere çözüm üretmeyi ve sağlık verisi güvenliğine yönelik açık risklere dikkat çekmeyi amaçlamaktadır.

Türkiye'de sağlık verisi güvenliği ile blokzincir entegrasyonunu birlikte ele alan az sayıdaki kapsamlı akademik çalışmalardan biri olarak, bu tezin hem literatüre hem de sektörel uygulamalara özgün katkılar sunması hedeflenmiştir.

Tez sürecinde, bilgi ve tecrübeleriyle her aşamada yol gösteren, kıymetli önerileri ve akademik rehberliğiyle çalışmanın bilimsel altyapısını güçlendiren danışmanım Sayın Prof. Dr. Mehmet Serdar GÜZEL'e en içten teşekkürlerimi sunuyorum. Bunun yanı sıra, hayatımın her döneminde olduğu gibi bu zorlu süreçte de bana güç ve motivasyon kaynağı olan oğullarım Eymen ve Ahmet Aras'a, desteğini hiçbir zaman esirgemeyen eşim Tuğba ÖZCAN'a ve her zaman yanımda hissettiğim aileme en derin teşekkürlerimi iletiyorum.

Eray ÖZCAN
Ankara, Eylül 2025

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

1.1 Genel Arka Plan

Sağlık sektörü, hasta verilerinin güvenli, bütünlük içinde ve yetkili kişilerle paylaşımını sağlama konusunda uzun yıllardır zorluklarla karşılaşmaktadır. Modern sağlık hizmetlerinin karmaşık yapısı ve çok paydaşlı ekosistemi göz önünde bulundurulduğunda, bu zorlukların boyutları daha da belirginleşmektedir. Geleneksel merkezi sistem mimarilerinde hasta bilgileri genellikle kurum özelinde sistemlerde tutulmakta ve farklı sağlık hizmet sağlayıcıları arasında gerçek zamanlı, güvenli veri paylaşımı oldukça sınırlı düzeyde gerçekleştirilebilmektedir. Bu durum, hastaneler, klinikler, laboratuvarlar ve diğer sağlık kurumları arasında bilgi akışının kesintiye uğramasına ve hasta tedavi kalitesinin olumsuz etkilenmesine neden olmaktadır. Kişisel sağlık verilerinin gizliliği, bütünlüğü ve yetkilendirme mekanizmaları konularında yaşanan eksiklikler hem hasta güvenliğini hem de sağlık hizmetlerinin etkinliğini olumsuz yönde etkilemektedir. Dijital dönüşümün her alanda hızla yaşandığı düşünüldüğünde; sağlık sektöründe, veri güvenliği ve ortak çalışabilirlik konuları daha da önem kazanmıştır.

Blokzincir teknolojisi, merkezi olmayan, değiştirilemez ve şeffaf yapısıyla sağlık bilgi sistemlerindeki bu problemlere kapsamlı çözümler üretme potansiyeline sahiptir. Bu teknolojinin dağıtık yapısı, tek bir merkezi otoriteye bağımlılığı ortadan kaldırarak sistem güvenilirliğini artırmaktadır. Hasta verilerinin kayıt altına alınması, doğrulanması, paylaşılması ve denetlenmesi süreçlerinde blokzincir tabanlı yaklaşımlar, geleneksel yöntemlere kıyasla daha yüksek güvenlik, şeffaflık ve veri bütünlüğü sağlama yeteneğine sahiptir. Bununla birlikte, blokzincir tabanlı sağlık sistemlerinin teknik uygulanabilirliği, performans gereksinimleri, ölçeklenebilirlik sorunları ve yasal uyumluluk boyutları henüz tam anlamıyla olgunlaşmış değildir ve bu alanda kapsamlı araştırmalara ihtiyaç duyulmaktadır.

Mevcut çalışmamız Hyperledger Fabric altyapısını kullanarak sağlık sektöründe kişisel sağlık kayıtlarının güvenli ve standartlara uygun şekilde yönetilmesi için kapsamlı bir

prototip modeli geliştirmeyi amaçlamaktadır. Hyperledger Fabric'in izinli ağ yapısı ve gelişmiş gizlilik koruma özellikleri, hasta verilerinin yetkisiz erişimlerden korunmasını sağlarken, aynı zamanda gerekli durumlarda yetkili sağlık profesyonellerinin bu verilere erişimini de mümkün kılmaktadır. Özellikle elektronik sağlık kayıtları (electronic health records - EHR) veri paylaşım standardı olan Hızlı Sağlık Hizmetleri Birlikte Çalışabilirlik Kaynakları (Fast Healthcare Interoperability Resources-FHIR) içerisinde oluşturulan uluslararası hasta özeti verilerini içeren uluslararası hasta özeti FHIR International Patient Summary (IPS) standartları ile entegrasyonu sayesinde farklı sağlık kurumları arasında birlikte çalışabilirlik desteklenmekte ve uluslararası sağlık veri paylaşım standartlarına uyumluluk sağlanmaktadır. Bu entegrasyon, elektronik sağlık kayıtlarının farklı sistem ve platformlar arasında sorunsuz bir şekilde paylaşılmasını sağlamakta ve hasta bakım sürekliliği de böylece korunmaktadır.

Geliştirilen sistem mimarisi, hasta mahremiyetini korurken aynı zamanda sağlık hizmet sağlayıcılarının ihtiyaç duydukları kritik bilgilere zamanında erişebilmelerini sağlamayı hedeflemektedir. Bu çerçevede, akıllı sözleşmeler kullanılarak veri erişim izinleri otomatik olarak yönetilmekte ve her bir veri paylaşım işlemi blokzincir üzerinde şeffaf bir şekilde kayıt altına alınmaktadır. Böylece sistem hem teknik hem de yasal gereksinimleri karşılayacak şekilde tasarlanmış olmaktadır.

Bu tez çalışması kapsamında bazı temel araştırma sorularına detaylı bir şekilde yanıt aranmaktadır: Blokzincir teknolojisi sağlık verilerinin güvenliğini, gizliliğini ve bütünlüğünü nasıl artırabilir? Bu teknolojinin sağlık sektörüne sağlayabileceği katma değerler nelerdir? Hyperledger Fabric altyapısı, sağlık sektörü özelinde FHIR IPS gibi uluslararası standartlara tam uyumlu bir şekilde veri paylaşımını destekleyebilir mi? Süreçte karşılaşılabilecek teknik zorluklar nelerdir? Sağlık blokzinciri sistemlerinin performans, ölçeklenebilirlik, veri gizliliği ve maliyet etkinliği açısından avantajları ve sınırlılıkları nelerdir? Bu sistemlerin pratik uygulanabilirliği hangi koşullarda mümkün olmaktadır? Bu sorular ışığında çalışmanın temel motivasyonu teorik analiz sonucunda şu şekilde tanımlanmıştır: Blokzincir tabanlı bir sağlık bilgi sistemi, geleneksel merkezi sistemlere kıyasla önemli ölçüde daha yüksek veri bütünlüğü, denetlenebilirlik ve güvenilirlik sunacaktır. Hyperledger Fabric altyapısı kullanılarak geliştirilen prototip

sistem, FHIR IPS standardı ile tam uyumlu hasta verilerinin güvenli, hızlı ve etkin şekilde paylaşımını başarılı bir şekilde sağlayabilecektir. Blokzincir yapısının sunduğu teknik avantajlar sayesinde farklı sağlık kurumları arasında güvenilir, izlenebilir, denetlenebilir ve gerçek zamanlı veri paylaşımı mümkün olacak ve bu durum hasta bakım ve tedavi kalitesinin artırılmasına önemli katkılar sağlayacaktır.

1.2 Tezin Amacı ve Kapsamı

Bu tez çalışmasının temel amacı, Hyperledger Fabric tabanlı bir blokzincir altyapısı üzerinde, uluslararası sağlık bilgi standartlarına uygun ve veri güvenliğini ön planda tutan bir prototip sistem geliştirmektir. Geliştirilen sistem ile sağlık hizmet sağlayıcıları, hastalar ve diğer paydaşlar arasında güvenilir, şeffaf ve kontrol edilebilir bir veri paylaşım ortamı oluşturulması hedeflenmektedir.

Çalışmanın önemi, blokzincir teknolojisinin sağlık sektörüne entegrasyonuna yönelik uygulamalı ve teknik bir katkı sunmasıdır. Özellikle Türkiye'de ve dünya genelinde sağlık verilerinin güvenliği, hasta mahremiyeti ve sistemler arası veri bütünlüğü gibi konuların kritik öneme sahip olduğu dikkate alındığında, bu araştırma mevcut bilgi birikimine yenilikçi bir bakış açısı kazandıracaktır. Ayrıca FHIR standardı kullanılarak oluşturulan yapının, uluslararası sağlık bilişim ekosistemi ile de uyumlu çalışması hedeflenmektedir.

1.3 Bölüm Yapısı

Bu tez beş bölümden oluşmaktadır. Her bölüm, çalışmanın temelinden uygulama detaylarına ve test sonuçlarına kadar farklı detaylara değinmektedir.

Birinci bölüm, araştırmanın genel çerçevesini sunmakta olup, sağlık bilgi sistemlerinde mevcut sorunların tanımlandığı, çalışmanın amaç ve kapsamının belirlendiği ve tezin genel organizasyonunun açıklandığı giriş kısmını içermektedir.

İkinci bölüm, konuyla ilgili literatürün özetlenmesi ve çalışmanın dayandığı temellerin açıklanması amacını taşımaktadır. Sağlık bilgi sistemlerinde veri yönetimine ilişkin

mevcut yaklaşımlar, blokzincir teknolojisinin temel ilkeleri, izinli/izinsiz blokzincir yapılarının karşılaştırılması ve Hyperledger Fabric çerçevesi de bu bölümde ele alınmaktadır.

Üçüncü bölüm, çalışmada kullanılan teknolojiler, geliştirilen sistemin mimarisi ve Hyperledger Fabric altyapısına ilişkin detayların yer aldığı materyal ve yöntem kısmıdır. Bu bölümde ayrıca FHIR R4 veri modelinin sisteme entegrasyonu ve özel veri koleksiyonlarının (Private Data Collections) uygulanmasına dair mimari ve teknik açıklamalara da yer verilmektedir.

Dördüncü bölüm, gerçekleştirilen uygulama sonrası elde edilen test bulguları içermekte ve analiz etmektedir. Zincir kodunun yaşam döngüsü, fonksiyonel doğrulama testleri, eşzamanlı erişim senaryoları ile veri güvenliği ve gizliliğine yönelik testler ayrıntılı olarak sunulmakta ve irdelenmektedir.

Beşinci bölüm, çalışmanın genel değerlendirmesinin yapıldığı, elde edilen bulgular doğrultusunda sonuçların tartışıldığı ve gelecekte yapılabilecek çalışmalara yönelik önerilerin sunulduğu son kısımdır.

2. KAYNAK ÖZETLERİ ve KURAMSAL TEMELLER

Bu bölümde, günümüzde sağlık bilgi sistemlerinin veriyi nasıl yönettiğine değinilerek, karşı karşıya kalınan temel sorunlar irdelenecektir. Günümüzde kullanılan merkezi sistemlerin yapısı, avantajları ve sınırlılıkları ele alınacaktır. Sağlık verisinin üretildiği andan itibaren, saklanması, işlenmesi ve paylaşılması aşamasında benimsenen yaklaşımlar değerlendirilecektir. Özellikle de veri bütünlüğü, erişim kontrolü, mahremiyet ve denetlenebilirlik üzerinden mevcut sistemlerin zafiyete sebep olma durumları üzerinde durulacaktır. Ardından, blokzincir teknolojisine ilişkin temel kavramlar sunularak, bu teknolojinin genel yapısı, dağıtık defter mimarisi, değiştirilemezlik özelliği ve kriptografik doğrulama mekanizmaları açıklanacaktır. Blokzincirin sunduğu teknik avantajların sağlık bilgi sistemlerinde nasıl karşılık bulabileceği irdelenecektir. Blokzincir teknolojisinin sağlık verisi yönetiminde uygulanabilirliğine ilişkin kavramsal altyapı üzerinde durulacaktır. Son olarak, bu teknolojinin temel yapı taşlarından biri olan akıllı sözleşmeler (smart contracts) ile izinli blokzincir (permissioned blockchain) kavramlarına da yer verilecektir. Akıllı sözleşmelerin işlem otomasyonu, veri doğrulama ve politika uygulama mekanizmaları olarak nasıl çalıştığı detaylandırılacak; izinli blokzincir yapısının erişim kontrolü ve düzenleyici uyum açısından sağladığı avantajlar ortaya konacaktır. Böylece, çalışmanın teknik temelini oluşturan blokzincir mimarisine dair teorik zemin oluşturulacaktır.

2.1 Sağlık Bilgi Sistemleri ve Veri Yönetiminde Mevcut Durum

Günümüz sağlık sistemlerinde hasta verilerinin dijital ortamlarda saklanması ve sistemler arası paylaşılması yaygın olarak uygulanmaktadır. Elektronik Sağlık Kayıtları (Electronic Health Records – EHR) ve Elektronik Hasta Kayıtları (Electronic Medical Records – EMR) sistemleri, sağlık kurumları arasında veri alışverişini mümkün kılmakta; ancak bu sistemlerin entegrasyonunda birtakım temel zorluklar ortaya çıkmaktadır. Farklı kurumsal altyapıların, standart dışı veri formatlarının ve birbirinden kopuk veri modellerinin varlığı, sistemler arası birlikte çalışabilirlik açısından önemli engeller oluşturmaktadır. Sağlık verilerinin yapısı gereği yüksek düzeyde hassasiyet içermesi, bu alandaki güvenlik risklerini daha da kritik hâle getirmektedir. Özellikle yetkisiz erişimler,

veri sızıntıları ya da kötüye kullanım durumları hem hasta mahremiyetini hem de veri güvenliğini ciddi şekilde tehdit etmektedir. Ayrıca sağlık sorunları ile ilgili olarak sunulan sigortacılıkta geri ödeme, sürücü belgesi, engelli hakları gibi bazı durumlarda sağlık durumunun belgelendirilmesini, raporlanmasını şart koşmaktadır. Ancak bu durumlarda sunulan belgelerde değiştirilebilirlik ve otorite eksikliği sahteciliğe ve dolandırıcılığa açık haldedir.

Mevcut sistemlerde hastaların kendi sağlık verileri üzerinde doğrudan kontrol sahibi olmamaları, kimlerle ve ne zaman paylaşıldığını şeffaf biçimde takip edememeleri önemli bir diğer eksikliktir. Bu durum, yalnızca teknik bir sorun olmaktan öte, etik ve yasal açılardan da hasta haklarını zedeleyen bir öneme sahiptir.

Tüm bu problemler, sağlık sektöründe daha şeffaf, güvenli ve hasta odaklı veri yönetimi yaklaşımlarının gerekliliğini ortaya koymaktadır. Özellikle, veri paylaşımlarının merkezi olmayan, izlenebilir ve denetlenebilir şekilde yönetilmesi, olası bir güvenlik ihlali veya adli analiz gerektiren bir olay durumunda geçmişe dönük işlem kayıtlarının doğrulanabilmesi büyük avantaj sağlayacaktır.

2.2 Blokzincir Teknolojisinin Temelleri

Blokzincir, verilerin merkezi bir otoriteye gerek duymadan, kriptografik olarak doğrulanabilir ve değiştirilemez biçimde saklanmasını sağlayan dağıtık defter teknolojisidir. (Nakamoto, 2008; Swan, 2015). Blokzincirin temel özellikleri şu şekilde özetlenebilir:

- Değiştirilemezlik: Bir kez kaydedilen veriler, kriptografik mekanizmalar sayesinde sonradan değiştirilemez veya silinemez (Crosby ve diğerleri, 2016).
- Şeffaflık ve İzlenebilirlik: Blokzincir üzerinde gerçekleşen tüm işlemler izlenebilir, böylece sistem denetlenebilir yapıdadır (Zyskind, Nathan ve Pentland, 2015).
- Merkeziyetsizlik: Geleneksel sistemlerin aksine, veriler tek bir merkezde değil, dağıtık şekilde birden fazla noktada tutulabilir (Tapscott ve Tapscott, 2016).

- Güvenli Yapı: Kriptografi tabanlı mekanizmalar, blokzincirin saldırılara karşı dayanıklı olmasını sağlar (Conti ve diğerleri, 2018).

Bu özellikler, sağlık alanında özellikle veri güvenliği, bütünlük ve izlenebilirlik konularında önemli avantajlar sunmaktadır (Mettler, 2016; Engelhardt, 2017).

2.3 İzinli ve İzinsiz Blokzincir Yapıları

Blokzincir sistemleri genel olarak izinli ve izinsiz olmak üzere iki temel kategoriye ayrılmaktadır (Crosby ve diğerleri, 2016; Tapscott ve Tapscott, 2016). İzinsiz blokzincir sistemleri, örneğin Bitcoin ve Ethereum gibi ağlar, tamamen açık yapıları sayesinde herkesin katılımına imkân tanıyan, merkeziyetsiz ve şeffaf sistemlerdir. Bu tür yapılarda tüm işlemler tüm katılımcılar tarafından görüntülenebilir, bu da sistemin güvenliğini ve değiştirilemezliğini artırırken mahremiyetin kısıtlanmasına yol açabilir (Nakamoto, 2008; Zyskind, Nathan ve Pentland, 2015).

Buna karşılık, izinli blokzincir sistemlerinde katılımcılar önceden belirlenir ve erişim yetkileri merkezi bir otorite veya konsorsiyum tarafından kontrol edilir (Swan, 2015; Mettler, 2016). Sağlık sektörü gibi yüksek düzeyde gizlilik, veri koruma ve düzenleyici uyumluluk gerektiren alanlarda, genellikle izinli blokzincir yapılarının tercih edildiği görülmektedir. Özellikle Hyperledger Fabric gibi kurumsal düzeyde izinli blokzincir platformları, sağlık sektörünün gerektirdiği veri gizliliği, erişim kontrolü ve düzenleyici uyumluluk ihtiyaçlarını karşılayan esnek ve güvenli bir altyapı sunmaktadır. (Androulaki ve diğerleri, 2018; Hyperledger Foundation, 2024).

İzinli blokzincir yapılarının sunduğu avantajlar arasında kimlik doğrulama ve yetkilendirme süreçlerinin etkin şekilde yönetilebilmesi, yüksek performans ve işlem kapasitesi sunulması ile verilerin yalnızca yetkilendirilmiş taraflarca görüntülenebilmesi öne çıkar. (Conti ve diğerleri, 2018; Engelhardt, 2017). Bu sayede, sağlık verisi gibi mahrem bilgilerin, sadece izin verilen kurumlar ve kişiler arasında güvenli biçimde paylaşılması mümkün olmaktadır.

2.4 Akıllı Sözleşmeler ve Zincir Üstü İşlemler

Akıllı sözleşmeler, blokzincir üzerinde çalışan, belirli koşulların gerçekleşmesi durumunda otomatik olarak devreye giren dijital protokoller olarak tanımlanmaktadır (Szabo, 1997; Christidis ve Devetsikiotis, 2016). Merkeziyetsiz yapıda çalışan bu sözleşmeler, aracıya ihtiyaç duymadan taraflar arasında güvenli, şeffaf ve otomatik işlem gerçekleştirilmesine olanak sağlamaktadır. Sağlık sektöründe akıllı sözleşmeler; hasta onamlarının dijital ortamda kaydedilmesi ve yönetilmesi, yetkilendirme ve erişim kontrolü mekanizmalarının uygulanması ile kurumlar arası veri paylaşımı süreçlerinin güvenliğinin artırılması gibi alanlarda önemli rol oynamaktadır (Mettler, 2016; Engelhardt, 2017).

Blokzincir altyapısında çalışan akıllı sözleşmeler sayesinde, sağlık verilerine erişim ancak önceden tanımlanmış kurallar ve hasta onamı çerçevesinde mümkün olmakta, bu da hem veri güvenliğini artırmakta hem de hasta mahremiyetini güçlendirmektedir (Zyskind, Nathan ve Pentland, 2015). Özellikle Hyperledger Fabric gibi izinli blokzincir platformları, zincir kodu (chaincode) adı verilen yapı üzerinden akıllı sözleşme geliştirilmesine olanak tanımaktadır (Androulaki ve diğerleri, 2018; Hyperledger Foundation, 2024). Zincir kodu, sistem üzerinde gerçekleşen işlemleri denetleyen ve önceden tanımlanan iş kurallarının otomatik olarak yürütülmesini sağlayan program parçalarıdır. Bu yapı sayesinde karmaşık sağlık iş akışlarının, özellikle veri paylaşımı, erişim kısıtlama ve onam yönetimi gibi süreçlerin, blokzincir üzerinde güvenli ve denetlenebilir şekilde uygulanması mümkün hale gelmektedir.

2.5 Sağlık Sektöründe Blokzincir Kullanımı ve Literatürdeki Yaklaşımlar

Son yıllarda sağlık alanında blokzincir tabanlı pek çok proje ve akademik araştırma yapılmıştır. Literatürde özellikle sağlık verilerinin bütünlüğünün sağlanması, sahtecilik girişimlerinin önlenmesi ve veri paylaşım süreçlerinin güvenli hale getirilmesi konularında blokzincir teknolojisinin sunduğu avantajlar ön plana çıkmaktadır (Azaria ve diğerleri, 2016; Engelhardt, 2017; Mettler, 2016). Blokzincirin sunduğu şeffaf ve değiştirilemez yapı sayesinde, hasta verilerinin doğruluğu garanti altına alınabilmekte,

yetkisiz erişim girişimleri engellenmekte ve tüm erişim kayıtları denetlenebilir şekilde tutulabilmektedir (Zyskind, Nathan ve Pentland, 2015). Ayrıca, blokzincir altyapısı hasta odaklı veri yönetimi anlayışını desteklemekte; bireylerin kendi sağlık verileri üzerindeki kontrolünü artırarak, kimin, ne zaman ve hangi amaçla verilere eriştiğini belirleme imkânı sunmaktadır (Dubovitskaya ve diğerleri, 2017; Engelhardt, 2017). Bununla birlikte, blokzincirin sağlık sektöründe yaygınlaştırılmasının önünde bazı önemli engeller de bulunmaktadır. Özellikle düzenleyici belirsizlikler, farklı ülkelerdeki yasal çerçevelerin uyumsuzluğu, teknolojinin ölçeklenebilirliği konusundaki sınırlılıklar ve mevcut sağlık bilgi sistemleriyle entegrasyonun karmaşıklığı, uygulama süreçlerinde önemli zorluklar yaratmaktadır (Agbo, Mahmoud ve Eklund, 2019; Mettler, 2016).

Bu çalışmada, söz konusu zorluklar dikkate alınarak izinli blokzincir altyapısı temelinde sağlık verilerinin güvenli, şeffaf ve hastayı odağa alacak biçimde işlenmesini sağlayan bir sistem tasarlanmış ve uygulanmıştır. Tasarım sürecinde, sağlık verilerinin yüksek gizlilik ihtiyacı, düzenleyici uyumluluk zorunlulukları (örneğin KVKK ve GDPR) ve veri bütünlüğü ihtiyaçları göz önünde bulundurulmuştur. Merkezi olmayan ancak erişim kontrollü bir yapı benimsenmiştir. Sistemin temel bileşenleri arasında kimlik yönetimi, erişim yetkilendirme, veri bütünlüğü doğrulama ve işlem kayıtlarının izlenebilirliği yer almaktadır. Prototip sistem, Hyperledger Fabric platformu üzerinde geliştirilmiştir. Bu platformun tercih edilme nedeni, modüler mimarisi, izinli katılım modeli, gelişmiş kimlik doğrulama (Membership Service Provider - MSP) altyapısı ve zincir kodu (chaincode) üzerinden özelleştirilebilir akıllı sözleşme desteği sunmasıdır. Sistem, gerçekçi uygulama senaryoları üzerinden test edilmiştir. Bu senaryolarda farklı paydaşlar (örneğin hastane, sigorta kurumu, laboratuvar ve hasta) arasında gerçekleştirilen veri erişim, paylaşım ve onam yönetimi işlemleri test edilmiştir. Elde edilen bulgular, blokzincir teknolojisinin sağlık verilerinin yönetimi açısından önemli potansiyel sunduğunu, özellikle veri bütünlüğü, izlenebilirlik ve güvenli paylaşım konularında mevcut sistemlere göre avantaj sağladığını göstermektedir. Aynı zamanda ölçeklenebilirlik, işlem hızı ve mevcut sağlık bilgi sistemleriyle entegrasyon gibi alanlarda geliştirilmeye açık yönlerin bulunduğu da belirtilmiştir. Bu yönü ile çalışmamız, blokzincir tabanlı sağlık bilgi sistemlerinin gerçek dünya koşullarında uygulanabilirliğini değerlendiren deneysel bir çalışma olup ileride yapılacak akademik ve kurumsal çalışmalara temel teşkil etmektedir.

3. MATERYAL ve YÖNTEM

3.1 Kullanılan Teknolojiler ve Araçlar

Bu çalışmada, blokzincir tabanlı sağlık veri yönetim sisteminin geliştirilmesi ve test edilmesi amacıyla bir test sistemi kurulmuştur. Tüm geliştirme ve test süreçleri için donanım altyapısı olarak 12. nesil Intel Core i7-1260P işlemci, 16 GB RAM ve 512 GB SSD depolama kapasitesine sahip bir bilgisayar kullanılmıştır. Yazılım tarafında, Hyperledger Fabric 2.5 sürümü tercih edilmiş ve sistem, Ubuntu 22.04 tabanlı bir WSL (Windows Subsystem for Linux) ortamında kurulmuştur. Geliştirme ve test aşamalarında Docker Engine (sürüm 24.0.7) ve Docker Compose (sürüm 2.24.7) bileşenleri aktif olarak kullanılmıştır. Hyperledger Fabric ağının kurulumu sırasında TLS (Transport Layer Security) tabanlı güvenli haberleşme konfigürasyonları uygulanmıştır.

Ayrıca, sistemdeki blokzincir ağına bağlı tüm düğümlerin kimlik yönetimi için Hyperledger Fabric CA (Certificate Authority) modülü kullanılmış, ağ katılımcılarının dijital kimlikleri ve sertifika altyapısı bu modül üzerinden yönetilmiştir. Akıllı sözleşme (chaincode) geliştirme sürecinde ise Go programlama dili ve Hyperledger Fabric Contract API (v1.2.1) kütüphanesinden yararlanılmıştır.

Yazılım geliştirme ve konfigürasyon yönetimi süreçlerinde Visual Studio Code, Git ve çeşitli terminal araçları kullanılmış, sistem üzerindeki tüm testler, ilgili senaryolara uygun olarak Docker konteynerleri üzerinde izole biçimde gerçekleştirilmiştir. Ayrıca ağın izlenmesi ve hata ayıklama süreçleri için Hyperledger Fabric'in sunduğu CLI araçları ve log kayıtlarından yararlanılmıştır.

3.2 Sistem Mimarisi ve Tasarım

Bu tez çalışmasında önerilen blokzincir tabanlı sağlık verisi yönetim sistemi, çok katmanlı ve modüler bir mimari anlayışla tasarlanmıştır. Mimari yapı, sağlık verilerinin güvenli, şeffaf, izlenebilir ve hasta odaklı bir şekilde yönetilmesini sağlayacak şekilde üç

temel katmandan oluşmaktadır. Bunlar blokzincir altyapı katmanı, akıllı sözleşme katmanı ve veri erişim katmanıdır.

İlk olarak Blokzincir Altyapı Katmanı sistemin temelini oluşturan Hyperledger Fabric tabanlı dağıtık ağ mimarisini içermektedir. İzinli (permissioned) bir blokzincir modeli tercih edilmiştir. Her sağlık kuruluşu (Örnek olarak hastane ve sigorta şirketi kullanılmıştır.) bağımsız bir organizasyon olarak tanımlanmış ve her birine özel birer *'peer node'* atanmıştır. Ağdaki tüm kuruluşlar, *"healthchannel"* isimli ortak bir kanal üzerinde işlem yapmakta ve işlemlerin bütünlüğü, MSP (Membership Service Provider) yapılandırmaları ile güvence altına alınmaktadır. Her peer node, hem blokzincir defterini hem de World State veritabanını (LevelDB) tutarak sistemin güncel ve geçmiş verilerini senkronize şekilde barındırmaktadır. Private Data Collections (PDC) mekanizması sayesinde, hassas hasta verileri sadece yetkili organizasyonlarda saklanırken, veri bütünlüğü özet tabanlı doğrulama (hash-based verification) ile tüm ağ tarafından doğrulanabilmektedir.

İkinci olarak; akıllı sözleşme katmanı, sistemdeki iş mantığının tanımlandığı ve otomatik olarak yürütüldüğü katmandır. JavaScript (Node.js) dilinde geliştirilen akıllı sözleşmeler (chaincode), Hyperledger Fabric Contract API kullanılarak yazılmıştır. Chaincode içerisinde FHIR R4 (Release 4) uyumlu sağlık veri yapıları, hasta kayıt yönetimi, özel veri koleksiyonları ile hassas veri koruması ve erişim kontrolü gibi temel işlevler tanımlanmıştır. Sistem, ikili depolama modeli (dual storage pattern) uygulayarak, demografik bilgileri LevelDB'de herkese açık şekilde tutarken, TC kimlik numarası gibi hassas verileri özel koleksiyonda sadece yetkili organizasyonların erişimine açık olarak saklamaktadır. Böylece, sistemdeki tüm işlemler güvenli, değiştirilemez ve otomatik kurallara dayalı bir şekilde yürütülmekte, hasta mahremiyeti ve erişim yetkileri kriptografik olarak denetlenebilir haldedir.

Son olarak Veri Erişim ve Yönetim Katmanı olarak tasarlanan katman farklı sağlık kuruluşları arasında güvenli veri paylaşımını ve yönetimini sağlayan ara yüz (interface) katmanıdır. Mevcut uygulamada, Hyperledger Fabric'in Komut Satırı Arayüzü (Command Line Interface - CLI) araçları kullanılarak chaincode (zincir kodu)

fonksiyonlarına erişim sağlanmaktadır. Bu yaklaşım, sistemin temel işlevselliğinin geliştirilmesi ve test edilmesi süreçlerinde kontrol sunarken, üretim ortamında web tabanlı arayüzlerle genişletilmeye uygun bir yapıya sahiptir. Veri erişim katmanı şu temel bileşenleri içermektedir:

- Erişim Kontrolü Mekanizması: Sistemde, MSP (Membership Service Provider) tabanlı kimlik yönetimi yapısı kullanılarak erişim kontrolü sağlanmaktadır. Erişim yetkilendirmesi; organizasyon kimliği, kullanıcı rolü ve işlem politikaları temel alınarak uygulanmaktadır. Bu yapı sayesinde, sağlık verilerinin mahremiyeti korunmakta ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemelere uyumluluk sağlanmaktadır.
- Veri Anonimleştirme Modülü: *"GetPatientPublic"* fonksiyonu aracılığıyla, hastalara ait verilerin anonimleştirilmiş versiyonlarına erişim imkânı sunulmaktadır. Bu modül, "ilk karakter koruma" temelli özel bir algoritma kullanarak, demografik verilerin faydasını korurken bireylerin doğrudan tanımlanma riskini azaltmaktadır. Böylece, verinin analitik amaçlarla kullanılabilirliği korunurken gizlilik ilkesi de dengeli şekilde uygulanmaktadır.
- Denetim ve İzlenebilirlik Sistemi: Tüm veri erişim ve değişiklik işlemleri, blokzincir üzerinde değiştirilemez işlem kayıtları (immutable transaction records) olarak tutulmaktadır. Bu sayede, geriye dönük tam izleme (comprehensive audit trail) ve inkâr edilemezlik (non-repudiation) gibi güvenlik özellikleri sağlanmaktadır. Her işlem, şeffaf ve denetlenebilir bir yapıda kaydedilmektedir.
- Birlikte Çalışabilirlik ve Standardizasyon: Veri yapıları, FHIR R4 International Patient Summary (IPS) standardına tam uyumlu şekilde modellenmiştir. Bu yaklaşım sayesinde, sağlık ekosisteminde farklı sistemler arasında veri alışverişi sağlanmakta ve birlikte çalışabilirlik (interoperability) ilkesine uygun bir veri akışı gerçekleştirilmektedir.

Bu üç katmanlı mimari yaklaşım; blokzincir teknolojisinin merkeziyetsizlik (decentralization) ve değiştirilemezlik (immutability) özelliklerini, sağlık alanının gizlilik ve yasal uyumluluk gereksinimlerinin dengeli biçimde birleştirildiği bir sağlık verisi yönetim sistemi sunmaktadır.

3.3 Hyperledger Fabric Ağ Konfigürasyonu

Sistemin temelini oluşturan Hyperledger Fabric ağı, izinli (permissioned) ve çok kuruluş eklenmesi olanak sağlayacak bir yapı üzerine kurulmuştur. Ağ konfigürasyonu, güvenli haberleşme, dijital kimlik yönetimi, işlem politikaları ve akıllı sözleşme dağıtımını kapsayan bir çerçeveye sahiptir. Bu bölümde, önerilen sistemin blokzincir altyapısına ilişkin temel yapı taşları ve geliştirme ortamındaki teknik bazı detaylar açıklanmaktadır.

3.4 Ağ Topolojisi ve Organizasyon Yapısı

FHIR IPS blokzincir sistemi, sağlık ekosisteminin gerçek hayattaki ihtiyaçlarını yansıtacak şekilde organizasyonlardan oluşturulmaya çalışılmıştır. Temelde üç bileşen üzerine modellenmiştir. Şekil 3.1 FHIR IPS Blokzincir ağ topolojisi ’nde gösterilen ağ topolojisi, her kuruluşun kendi peer node’u, MSP (Membership Service Provider) yapılandırması ve erişim politikaları ile bağımsız şekilde çalışmasına olanak tanımaktadır.

```
erayc@DESKTOP-L0B76P7:~/fabric-test$ docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Status}}\t{{.Ports}}"
NAMES                       IMAGE                           STATUS          PORTS
peer0.insurance.health.com  hyperledger/fabric-peer:2.5     Up 4 seconds    7051/tcp, 0.0.0.0:8051->8051/tcp, [::]:8051->805
1/tcp
cli                         hyperledger/fabric-tools:2.5    Up 4 seconds
orderer.health.com          hyperledger/fabric-orderer:2.5  Up 5 seconds    0.0.0.0:7050->7050/tcp, [::]:7050->7050/tcp
peer0.hospital.health.com   hyperledger/fabric-peer:2.5     Up 5 seconds    0.0.0.0:7051->7051/tcp, [::]:7051->7051/tcp
erayc@DESKTOP-L0B76P7:~/fabric-test$
```

Şekil 3.1 FHIR IPS Blokzincir ağ topolojisi

Sistemde tanımlanan bileşenler şu şekildedir:

- *HospitalMSP (Hospital.health.com),* sistemde birincil sağlık hizmet sağlayıcısı (primary healthcare provider) rolünde yer almakta ve hastaya ait verilerin tam yetkili sahibi olarak bulunmaktadır. Bu organizasyona ait düğüm (peer node), *peer0.hospital.health.com:7051* adresinde çalışmakta olup, MSP dizin yapısı */crypto-config/peerOrganizations/hospital.health.com/msp* konumunda bulunmaktadır. HospitalMSP, tam hasta verisi üzerinde okuma ve yazma yetkilerine sahiptir ve aynı

zamanda sistemin anchor peer (çapa düğüm) bileşeni olarak, diğer organizasyonlarla yapılan iletişimin koordinasyonundan sorumludur.

- *InsuranceMSP (Insurance.health.com),* sistemde ikincil sağlık paydaşı (secondary healthcare stakeholder) olarak konumlanmakta ve yalnızca anonimleştirilmiş hasta verilerine erişim hakkına sahiptir. Bu organizasyona ait peer node, *peer0.insurance.health.com:8051* adresinde çalışmakta; MSP dizin yapısı ise */crypto-config/peerOrganizations/insurance.health.com/msp* konumunda yer almaktadır. InsuranceMSP, hasta mahremiyetini korumak amacıyla sadece anonimleştirilmiş (public) hasta verilerine erişebilmektedir; özel veri koleksiyonlarına (örneğin T.C. kimlik numarası gibi hassas alanlar) erişim izni bulunmamaktadır.

- *OrdererMSP*, Hyperledger Fabric ağında işlem sıralama (ordering) ve konse nsüs yönetimi (uzlaşma mekanizması) görevlerini üstlenen bileşeni temsil eder. Bu bileşen, ağ üzerindeki tüm işlemleri kronolojik sıraya koyarak bloklar halinde düzenler. İşlemlerin ağdaki tüm *peer* düğümlerine tutarlı biçimde dağıtılmasını sağlar. Orderer katmanı, sistemin doğruluk (consistency) ve bütünlük (integrity) ilkelerini koruması açısından oldukça önemlidir. OrdererMSP (Membership Service Provider) bileşeni ise bu katmandaki düğümlerin kimlik doğrulamasını, yetkilendirmesini ve güvenli iletişimini yönetir. Böylece sadece yetkili kuruluşların blok üretim sürecine katılmasına izin verilir. OrdererMSP'nin rolü, işlemlerin güvenilir biçimde sıralanmasını ve ağın tamamında tek bir doğrulanmış işlem geçmişi (ledger state) oluşturulmasını sağlamaktır. Bu sayede hem verilerin değiştirilemezliği korunur hem de sistem genelinde denetlenebilir bir işlem akışı oluşmuş olur.

- *CLI Ortamı (CLI Environment),* ağ yönetimi (network administration) ve akıllı sözleşme yönetimi (chaincode management) görevlerini yerine getirmektedir. Bu ortam, hyperledger/fabric-tools:2.5 imajı üzerinde çalışan bir konteyner aracılığıyla çalıştırılmakta olup, dinamik MSP geçiş yeteneği özelliğine sahiptir. Kısaca; CLI ortamı üzerinden gerçekleştirilen temel işlemler arasında, chaincode yükleme, test etme ve ağ izleme (monitoring) gibi işlevler yer almaktadır. Bu yapı sayesinde sistem yöneticileri, farklı kuruluşların işlem gerçekleştirme esnekliğine sahip olmakta ve ağın genel durumunu takip edebilmektedir.

Bu üç bileşenden oluşan yapı, sağlık alanının gerektirdiği çok paydaşlı ekosistemi ve kontrollü erişim ilkelerini dengeli bir şekilde karşılamaktadır. HospitalMSP'nin tam veri sahipliği, InsuranceMSP'nin kontrollü anonim erişimi, CLI Ortamı'nın ise teknik yönetim işlevlerini üstlenmesiyle sistem hem güvenli hem de birlikte çalışabilir bir mimari sunmaktadır. Bu mimari, sağlık sektöründe sıklıkla karşılaşılan veri paylaşımı, hasta onamı ve erişim kontrolü gibi karmaşık süreçlerin dağıtık ancak yönetilebilir bir biçimde yürütülmesine olanak sağlayacaktır. Ayrıca, her kuruluşun kendi düğümleri üzerinden bağımsız olarak işlem yapabilmesi hem veri mahremiyetinin korunmasını hem de sistemin ölçeklenebilirliğini artırmaktadır. Özetle, FHIR IPS blokzincir sisteminin ağ yapısı çok paydaşlı sağlık sistemi gereksinimlerine göre tasarlanmış olup, her organizasyonun ağ içinde tanımlı sorumluluk ve erişim sınırlarına sahip olmasını sağlamaktadır. Çizelge 3.1 FHIR IPS Blokzincir network bileşenleri'nde detayları gösterilen yapımız, organizasyonların kendi eş düğümleri ve erişim yetkileriyle bağımsız ancak birbirleri ile koordineli biçimde çalışabilmesini mümkün kılmaktadır.

Çizelge 3.1 FHIR IPS Blokzincir network bileşenleri

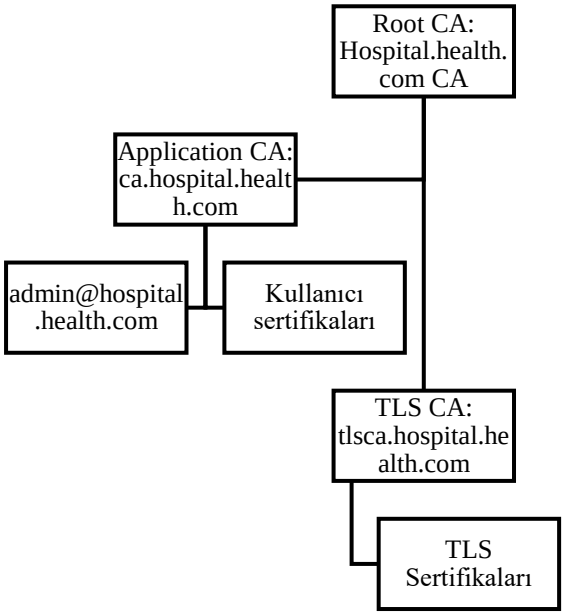
Organizasyon/MSP Kimliği	**Port**	**Rol**	**Veri Erişim Yetkisi**
HospitalMSP *peer0.hospital.health.com*	7051	Birincil Sağlık Hizmet Sunucusu	Hasta verilerinin tamamı ve özel veri koleksiyonları erişimi
InsuranceMSP *peer0.insurance.health.com*	8051	İkincil Sağlık Paydaşı	Yalnızca anonimleştirilmiş hasta verisine erişim
OrdererMSP *orderer.health.com*	7050	İşlem Sıralama Servisi	Ağ üzerindeki uzlaşma (konsensüs) mekanizmasının yönetimi
CLI Environment *cli*	-	Ağ Yönetimi	Dinamik MSP geçiş yeteneği

3.5 MSP Konfigürasyonu

MSP **(**Membership Service Provider- Üyelik Hizmet Sağlayıcısı**)** yapılandırması, ağın güvenlik temelini oluşturmakta ve her organizasyonun dijital kimlik yönetimini sağlamaktadır. Şekil 3.2 MSP dizin yapısı 'nda detaylı olarak gösterilen MSP dizin yapısı, X.509 sertifika ve rol tabanlı erişim kontrolü temeline dayanmaktadır. Her kuruluşa ait dijital kimlik altyapısı, Fabric CA tarafından oluşturulan X.509 sertifikalarla tanımlanmış ve bu sertifikalar MSP (Membership Service Provider) klasörlerinde saklanmıştır. MSP dizin yapısı, hospital.health.com organizasyonu için şu şekilde organize edilmiştir: admincerts klasörü yönetici (aministrator) sertifikaları, cacerts klasörü sertifika makamı (Certificate Authority) kök sertifikaları, *config.yaml* dosyası MSP yapılandırma parametreleri, keystore klasörü şifreli özel anahtarlar, signcerts klasörü imzalama sertifikaları ve tlscacerts klasörü TLS sertifikaları barındırmaktadır.

Şekil 3.2 MSP dizin yapısı

Sertifika hiyerarşisi ve güven zinciri (trust chain) yapısı *Şekil 3.3 Sertifika hiyerarşisi ve güven zinciri*'nde gösterildiği şekilde kurgulanmıştır. Root CA (Kök Sertifika Otoritesi) olarak Hospital.health.com CA sertifika makamı olarak işlev görmekte, Uygulama Sertifika Otoritesi (Application CA) olarak ca.hospital.health.com, blokzincir ağında için kimlik (identity) sertifikaları verme işlemlerini gerçekleştirmektedir. TLS CA (TLS Sertifika Otoritesi) olarak tlsca.hospital.health.com ise güvenli iletişim kanalı kurulumu için kullanılmaktadır. Sertifika detayları Şekil 3.4 MSP sertifikaları şeklinde görülebilir.



Şekil 3.3 Sertifika hiyerarşisi ve güven zinciri

```
erayo@DESKTOP-L0B76P7:~/fabric-test$ openssl x509 -in ~/fabric-test/crypto-config/peerOrganizations/hospital.health.com/msp/c
acerts/ca.hospital.health.com-cert.pem -noout -subject -issuer -dates -serial
subject=C = US, ST = California, L = San Francisco, O = hospital.health.com, CN = ca.hospital.health.com
issuer=C = US, ST = California, L = San Francisco, O = hospital.health.com, CN = ca.hospital.health.com
notBefore=Jun 28 21:40:00 2025 GMT
notAfter=Jun 26 21:40:00 2035 GMT
serial=8428A6DBB6B868CE3381AF9983DB891
erayo@DESKTOP-L0B76P7:~/fabric-test$ openssl x509 -in /home/erayo/fabric-test/crypto-config/peerOrganizations/hospital.health
.com/users/Admin@hospital.health.com/msp/signcerts/Admin@hospital.health.com-cert.pem -noout -subject -issuer -dates -serial
subject=C = US, ST = California, L = San Francisco, OU = admin, CN = Admin@hospital.health.com
issuer=C = US, ST = California, L = San Francisco, O = hospital.health.com, CN = ca.hospital.health.com
notBefore=Jun 28 21:40:00 2025 GMT
notAfter=Jun 26 21:40:00 2035 GMT
serial=FD5A5AC1858CD4DF4BA7D68148EF543A
erayo@DESKTOP-L0B76P7:~/fabric-test$ openssl x509 -in ~/fabric-test/crypto-config/peerOrganizations/hospital.health.com/msp/t
lscacerts/tlsca.hospital.health.com-cert.pem -noout -subject -issuer -dates -serial
subject=C = US, ST = California, L = San Francisco, O = hospital.health.com, CN = tlsca.hospital.health.com
issuer=C = US, ST = California, L = San Francisco, O = hospital.health.com, CN = tlsca.hospital.health.com
notBefore=Jun 28 21:40:00 2025 GMT
notAfter=Jun 26 21:40:00 2035 GMT
serial=7AE6E3B2DDC4C368F1ACF75D19D8583F
erayo@DESKTOP-L0B76P7:~/fabric-test$
```

Şekil 3.4 MSP sertifikaları

Bu yapı, blokzincir ağında katılımcı kimlik doğrulama, yetkilendirme ve güvenli iletişim gereksinimlerini karşılayarak, sağlık verilerinin korunması için gerekli kriptografik altyapıyı sağlamaktadır. Şekil 3.4' de görüldüğü üzere, her organizasyonun kendi MSP yapısına sahip olması, çok kuruluşlu sağlık ekosisteminde bağımsız kimlik yönetimi ve erişim kontrolü imkânı sağlamaktadır. Ek olarak *configtx.yaml* dosyasında tanımlanan "Policies" kuralları, kuruluş içinde kimlerin okuma, yazma ve yönetici yetkilerine sahip

olacağını belirlemektedir. Ayrıca tanımlanan anchor peer, kuruluşlar arası iletişimi sağlayan özel node olarak işlev görmektedir.

3.6 Ağ kuruluşları ve eş düğüm sunucusu konfigürasyonu

Ağda her sağlık kurumu bağımsız bir kuruluş (organization) olarak modellenmiş ve her birine ait bir adet eş düğüm sunucusu (peer node) yapılandırılmıştır. Her kuruluş, configtx.yaml dosyası aracılığıyla sistem profiline dahil edilmiştir (Şekil 3.5). Eş düğüm sunucuları, World State veritabanını (LevelDB) ve blokzincir defterini (ledger) tutarak hem güncel hem de geçmiş sağlık kayıtlarını senkronize biçimde barındırmaktadır.

Ubuntu > home > erayo > fabric-test > ! configtx.yaml

```
Organizations:
  - &OrdererOrg
    OrdererEndpoints:
      - orderer.health.com:7050

  - &HospitalMSP
    Name: HospitalMSP
    ID: HospitalMSP
    MSPDir: ./crypto-config/peerOrganizations/hospital.health.com/msp
    Policies:
      Readers:
        Type: Signature
        Rule: "OR('HospitalMSP.admin', 'HospitalMSP.peer', 'HospitalMSP.client')"
      Writers:
        Type: Signature
        Rule: "OR('HospitalMSP.admin', 'HospitalMSP.client')"
      Admins:
        Type: Signature
        Rule: "OR('HospitalMSP.admin')"
      Endorsement:
        Type: Signature
        Rule: "OR('HospitalMSP.peer')"
    AnchorPeers:
      - Host: peer0.hospital.health.com
        Port: 7051
```

Şekil 3.5 Hospital kuruluşunun organizasyon tanımı (configtx.yaml)

3.7 Kanal (Channel) yapılandırması

Hyperledger Fabric ağı içerisinde kanal (channel) yapılandırması, katılımcı kuruluşlar arasında güvenli ve izole bir işlem ortamı oluşturur. Sağlık alanının gerektirdiği veri gizliliği ve yasal uyumluluk koşullarını karşılamak amacıyla, kanal seviyesinde erişim

kontrolü ve işlem doğrulama mekanizmaları uygulanmaktadır. *'healthchannel'* isimli uygulama kanalımız, sağlık verilerine ilişkin tüm işlemler için özel ve güvenli bir iletişim yolu sağlamaktadır. Şekil 3.6 Kanal bilgileri' nde gösterilen healthchannel, işlemlerin onaylanması, sıralanması ve blokzincir defterine kaydedilmesi süreçlerinde kullanılmıştır.

Şekil 3.6 Kanal bilgileri

Kanalın başlangıç yapılandırması (genesis konfigürasyonu), ağın temel parametrelerini ve yönetim politikalarını tanımlar. Genesis bloğu, kanalın ilk durumunu belirleyerek sonraki işlem blokları için temel oluşturur; bu sayede defterin bütünlüğü ve işlemlerin kronolojik sıralaması güvence altına alınır. Genesis konfigürasyonu, ağdaki tüm kuruluşların kimlik doğrulama (MSP), politika tanımlama ve yetkilendirme mekanizmalarının başlangıçta senkronize biçimde oluşturulmasını sağlar. Bu aşamada tanımlanan politikalar, daha sonraki bloklarda yapılacak güncellemelerin veya yeni üyelerin kanala eklenmesinin hangi koşullarda gerçekleşeceğini belirler.

Şekil 3.7 Kanal başlangıç konfigürasyonu 'nda gösterilen configtx.yaml dosyası, OrdererOrg ve HospitalMSP organizasyonlarının MSP policies (MSP politikaları), erişim kontrol kuralları (Access control rules) ve orderer uç noktaları (endpoints) konfigürasyonunu içermektedir. Genesis bloğu kanalın başlangıç durumunu oluşturarak, sonraki işlem blokları için temel sağlamaktadır. Bu yapı, blokzincirin bütünlük, izlenebilirlik ve kronolojik sıralama özelliklerini garanti etmektedir.

```
erayo@DESKTOP-L0B76P7:~/fabric-test$ cat ~/fabric-test/configtx.yaml | head -30
Organizations:
  - &OrdererOrg
    Name: OrdererOrg
    ID: OrdererMSP
    MSPDir: ./crypto-config/ordererOrganizations/health.com/msp
    Policies:
      Readers:
        Type: Signature
        Rule: "OR('OrdererMSP.member')"
      Writers:
        Type: Signature
        Rule: "OR('OrdererMSP.member')"
      Admins:
        Type: Signature
        Rule: "OR('OrdererMSP.admin')"
    OrdererEndpoints:
      - orderer.health.com:7050

  - &HospitalMSP
    Name: HospitalMSP
    ID: HospitalMSP
    MSPDir: ./crypto-config/peerOrganizations/hospital.health.com/msp
    Policies:
      Readers:
        Type: Signature
        Rule: "OR('HospitalMSP.admin', 'HospitalMSP.peer', 'HospitalMSP.client')"
      Writers:
        Type: Signature
        Rule: "OR('HospitalMSP.admin', 'HospitalMSP.client')"
      Admins:
```

Şekil 3.7 Kanal başlangıç konfigürasyonu

Sağlık işlemlerinin kanal üzerindeki tipik akışı şu adımlardan oluşur: İstemci tarafından oluşturulan işlem teklifi, yetkili bir eş düğüm sunucusuna iletilir; burada akıllı sözleşme çalıştırılır ve varsa özel veriler ayrıştırılır. Ardından, dijital olarak imzalanmış onay yanıtı istemciye gönderilir. Bu işlem, sıralama için orderer node'una iletilir. Konsensüs mekanizması ile blok oluşturulup tüm eş düğüm sunucularına dağıtılır, defter güncellenir ve işlem tamamlandığında olay bildirimi yapılır.

3.8 Blokzincir Defteri ve LevelDB Yönetimi

Hyperledger Fabric mimarisinde blokzincir defteri (blockhain ledger), sistemin değiştirilemez işlem (transaction) geçmişi ve güncel durum bilgilerini barındıran bileşendir. Veri bütünlüğü, denetlenebilirlik ve inkâr edilemezlik özelliklerinin sağlanması, defter yapısının doğru tasarlanması ile sağlanmaktadır.

FHIR IPS sisteminde kullanılan defter yapısı, iki temel katmandan oluşmaktadır: blokzincir katmanı (blockchain layer) ve dünya durumu veritabanı (World State database). Blokzincir katmanında, geçmişe dönük tüm işlemler değiştirilemez bloklar hâlinde saklanırken; World State veritabanında, sistemin en güncel durumu anahtar–değer (key–value) çiftleri biçiminde tutulmaktadır. Bu iki katmanın birlikte kullanılması, sağlık verilerinin hem geçmiş versiyonlarının izlenebilmesini hem de gerçek zamanlı erişim gereksinimlerinin karşılanmasını sağlamaktadır. Böylece hasta kayıtları, tıbbi işlemler veya onam bilgileri gibi veriler hem geçmişteki haliyle denetlenebilir kalmakta hem de güncel duruma anında erişilebilmektedir.

Blokzincir defterinin temel yapısı, kronolojik olarak sıralanmış bloklar zincirinden oluşmaktadır. Her blok, kendisinden önceki bloğa ait bir hash değeri (previous block hash), işlem verilerini (transaction data) ve blok meta verilerini (block metadata) içermektedir. Bu yapı, defterin bütünlüğünü ve doğrulanabilirliğini koruyan kriptografik bir bağ oluşturur. Şekil 3.8 Blokzincir defter yapısı'nda, healthchannel kanalında yer alan blokzincir defteri görülebilir. Defterin mevcut yüksekliği *"Height: 9"* değeri ile ifade edilmekte olup, bu da sistemde toplam dokuz bloğun oluşturulduğunu göstermektedir. *currentBlockHash* ve *previousBlockHash* değerleri, her blok arasında kurulan kriptografik bağı temsil eder ve defterin kriptografik bütünlüğünü güvence altına alır. Her bir özet değeri, sağlık verilerinin herhangi bir şekilde değiştirilemeyeceğini ve tüm kayıtların doğrulanabilir biçimde korunduğunu göstermektedir. Bu mimari, sağlık alanında veri bütünlüğü, izlenebilirlik ve denetlenebilirlik ilkelerini desteklemekte; FHIR IPS tabanlı blokzincir sisteminin güvenli, şeffaf ve sürdürülebilir bir veri yönetim altyapısı sunmasına olanak sağlamaktadır. Ayrıca, değiştirilemez blok yapısı sayesinde hasta verileri üzerinde yapılan tüm işlemler kronolojik olarak geriye dönük incelenebilmekte, böylece tıbbi kayıtların şeffaflığı ve kurumsal hesap verebilirlik en üst düzeyde sağlanmaktadır.

Şekil 3.8 Blokzincir defter yapısı

Şekil 3.9 Mevcut verilerin görünümü (World State DB) ’de gösterilen World State yapısı, sistemdeki en güncel veri durumunu temsil etmektedir. Bu yapıda, hasta kimlik numaraları (patient ID) birer anahtar (key) olarak, bu kimliklere karşılık gelen FHIR R4 uyumlu JSON belgeleri ise değer (value) olarak saklanmaktadır. Böylece her bir hasta kaydı, blokzincir üzerinde güvenli biçimde kimliklendirilen ve en son güncellenmiş hâlini yansıtan bir veri çiftine dönüştürülmektedir. Bu yaklaşım, World State veritabanı sayesinde, karmaşık sorguların (örneğin belirli hastaya ait tüm laboratuvar sonuçları, alerji kayıtları veya reçeteler) anlık olarak yapılabilmesini de mümkün kılar. Veriler, JSON formatında tutulduğu için FHIR standartlarıyla doğrudan uyumlu bir yapı vardır. Bu mimari sayesinde sağlık kuruluşları, hasta verilerini güvenli biçimde saklarken aynı zamanda yüksek erişilebilirlik, sorgu performansı ve birlikte çalışabilirlik avantajı elde edecektir.

Şekil 3.9 Mevcut verilerin görünümü (World State DB)

Özel Veri Koleksiyonları (Private Data Collections- PDC), hassas sağlık verilerinin yönetimi için özel bir saklama mekanizması sunmaktadır. T.C. kimlik numarası gibi yüksek düzeyde gizlilik gerektiren veriler, World State'ten fiziksel olarak ayrı konumlanan özel koleksiyonlarda tutulurken; bu verilerin varlığına dair kanıt olarak SHA-256 hash değerleri genel blokzincir defterine kaydedilmektedir. Bu hibrit saklama modeli, blokzincirin şeffaf yapısıyla sağlık alanının mahremiyet gereksinimleri arasında

denge sağlayarak, sıfır bilgi ispatı (zero-knowledge proof) benzeri bir doğrulama yeteneği sunmaktadır. Özel verilerin gerçek içeriğine yalnızca yetkilendirilmiş kuruluşlar (örneğin HospitalMSP) erişebilirken, verinin bütünlüğü tüm ağ katılımcıları tarafından kriptografik olarak doğrulanabilmektedir. Veri saklama yapısı şu şekilde özetlenebilir:

- Genel Defter (Public Ledger): Hash değerleri ve ilişkili metadata bilgileri
- Özel Koleksiyon (Private Collection): Gerçek hassas veri içeriği
- Çapraz Referans (Cross-Reference): Kriptografik varlık kanıtı

3.9 İşlem Yaşam Döngüsü ve Defter Güncellemeleri

Sağlık işlemlerinin blokzincir defterine kaydedilme süreci, çok aşamalı bir doğrulama hattı üzerinden gerçekleşmektedir. Bu süreçte, hasta verilerinin bütünlüğünü ve sistem güvenilirliğini sağlamak amacıyla düzenli bir yaklaşım uygulanmıştır. *CreatePatient* adlı bir sağlık işleminin tam yaşam döngüsü aşağıdaki adımlar ile yürütülmektedir:

1. **İşlem Teklifi (Transaction Proposal):** İlk aşamada istemci (client), işlem teklifini yetkilendirilmiş bir eş düğüme iletir ve zincir kodu çalıştırma süreci başlatılır. Bu aşamada FHIR R4 uyumlu hasta verisi, ikili depolama modeli (dual storage pattern) gereğince genel (public) ve özel (private) bileşenlerine ayrıştırılır.
2. **Onaylama Süreci (Endorsement):** Eş düğümler, zincir kodunun çıktısını dijital imza ile doğrulayarak bir onaylama (endorsement) yanıtı üretir. Tek organizasyonlu ağ yapılarında (örneğin HospitalMSP), bu onaylama işlemi otomatik sağlanırken; çoklu organizasyon senaryolarında birden fazla eş düğüm sunucusunun onayı gerekebilir. Şekil 3.10'te gösterilen örnekte, PATIENT004 kaydının 789817…….28b6250778dca2f0 işlem kimliği ile başarıyla oluşturulduğu görülmektedir.
3. **İşlem Sıralama (Transaction Ordering):** Bu aşamada, orderer node onaylanmış işlemleri uzlaşı mekanizması ile işler ve kronolojik sıralamayı sağlar. Uygulamada Solo algoritması tercih edilmiş olup, işlem sıralama süreci tek bir orderer üzerinden yürütülmektedir.

4. **Blok Oluşturma (Block Formation):** Birden fazla sağlık işlemi bir blok içinde gruplanarak toplu işleme (batch processing) tabi tutulur. Blok boyutu ve işlem sayısı, sağlık süreçlerinin performans ihtiyaçlarına uygun şekilde ayarlanmış; böylece verimli veri işleme ve düşük gecikme (latency) dengesi sağlanmıştır.

5. **Deftere Kaydetme (Ledger Commit):** Oluşturulan blok, blokzincir defterine değiştirilemez kaydolarak eklenir ve kriptografik hash zinciri (hash chain) ile önceki bloklara bağlanır. Bu aşamada işlem verisi kalıcı olarak saklanır.

6. **Mevcut Durum Güncellemesi (World State Update):** Mevcut sistem durumu (current state), LevelDB veritabanında güncellenir. Örneğin, Şekil 3.10 'nda gösterildiği üzere blok yüksekliği 9'dan 10'a çıkmakta; PATIENT004 kaydı World State üzerinden erişilebilir hale gelmekte ve özel veri hash'i oluşturulmaktadır. Bu aşamada, gizlilik korumalı erişim sağlamak amacıyla anonimleştirme algoritmaları uygulanır.

7. **Olay Bildirimi (Event Notification):** İşlemin başarıyla tamamlandığına dair bildirim (event) istemciye yayınlanır. Bu mekanizma, sağlık uygulamalarının gerçek zamanlı işlem durumu takibi (real-time transaction status tracking) yapabilmesini sağlar.

Bu işlem yaşam döngüsünün her aşaması, sağlık sektöründe kritik öneme sahip ACID özelliklerini (Atomiklik, Tutarlılık, İzolasyon, Kalıcılık) koruyacak şekilde tasarlanmış olup, hasta verilerinin bütünlüğünü ve güvenilirliğini sağlamaktadır. (Şekil 3.11 İşlem doğrulama ve mevcut durum güncelleme)

Şekil 3.10 Hasta oluşturma işlemi ve onay süreci

Şekil 3.11 İşlem doğrulama ve mevcut durum güncelleme

3.10 FHIR IPS Akıllı Sözleşme Uygulaması

Bu çalışmada tasarlanan blokzincir tabanlı sağlık veri yönetim sisteminde, ağ üzerindeki işlem mantığı ve veri bütünlüğü akıllı sözleşmeler (smart contracts) aracılığıyla sağlanmaktadır. Hyperledger Fabric mimarisinde bu sözleşmeler, “chaincode” adı verilen bileşenler olarak tanımlanmakta ve her işlemin kurallara uygun olarak yürütülmesini sağlamaktadır. Sistemdeki chaincode yapısı, hasta verilerinin tanımlanması, kayıt altına

alınması, onam süreçlerinin yönetilmesi ve veri erişim taleplerinin kontrolü gibi temel fonksiyonları içermektedir. Chaincode'lar, Fabric Contract API kullanılarak Go diliyle geliştirilmiş ve FHIR standardı ile uyumlu veri yapıları esas alınarak modellenmiştir.

3.11 FHIR R4 Veri Modeli Entegrasyonu

Bu katmanda, FHIR R4 standardına uygun kaynak tanımlamaları yer almaktadır. Sistem, uluslararası hasta özeti (International Patient Summary - IPS) profilinde tanımlı temel kaynakları desteklemekte ve her kaynak için gelişmiş üst veri (metadata) desteği sağlamaktadır. Şekil 3.12' de gösterilen veri modeli yapısı, FHIR R4 standardının IPS profiline uygun olarak tasarlanmıştır. Bu model, sağlık verilerinin blokzincir ortamında standartlara uygun biçimde saklanmasını mümkün kılmaktadır. Patient (Hasta) Yapısı, hastaya ait demografik bilgiler ile Türkiye Cumhuriyeti Kimlik Numarası gibi tanımlayıcı bilgileri içermektedir. FHIR standardına uygun olarak kaynak türü (resourceType), kimlik (id), tanımlayıcı (identifier), ad-soyad (name), cinsiyet (gender) ve doğum tarihi (birthDate) gibi alanlar bu yapıda yer almaktadır. Alerji Bilgisi (AllergyIntolerance) Yapısı, hastanın alerjilerine ilişkin verileri SNOMED CT kodları ile temsil etmekte olup, kod (code) ve klinik durumu (clinicalStatus) gibi alanları içermektedir.

Bu yapı, FHIR terminoloji eşleştirme kurallarına tam uyum göstermektedir. Üst Veri (Metadata) Yapısı, blokzincir ortamında sürüm kontrolü (versioning) ve izlenebilirlik (audit trail) sağlamak amacıyla sürüm numarası (versionId), son güncelleme tarihi (lastUpdated) ve veri kaynağı (source) bilgilerini içermektedir. IPS Paket Yapısı (Bundle Container), hastaya ait tüm klinik verilerin tek bir FHIR belgesi (document) içerisinde toplanmasını sağlar. Bu yapı, IPS standardına uygun olarak "document" türünde organize edilmiştir. Söz konusu veri modeli, HL7 FHIR IPS Uygulama Kılavuzu (v1.1.0) ile tam uyumlu olup, JSON formatında serileştirme (serialization) ile farklı platformlar arasında veri paylaşımını ve birlikte çalışabilirliği desteklemektedir.

```
==========================================
    FHIR IPS BLOCKCHAIN DATA MODEL
==========================================

>>> CORE PATIENT RESOURCE <<<
type Patient struct {
        ResourceType string      `json:"resourceType"`
        ID           string      `json:"id"`
        Identifier   []Identifier `json:"identifier"`
        Name         []HumanName `json:"name"`
        Gender       string      `json:"gender"`
        BirthDate    string      `json:"birthDate"`
        Meta         Meta        `json:"meta"`
}

>>> CLINICAL DATA RESOURCES <<<
type AllergyIntolerance struct {
        ResourceType    string          `json:"resourceType"`
        ID              string          `json:"id"`
        Patient         Reference       `json:"patient"`
        Code            CodeableConcept `json:"code"`
        ClinicalStatus  CodeableConcept `json:"clinicalStatus"`
        Severity        string          `json:"severity,omitempty"`
        RecordedDate    string          `json:"recordedDate"`
        Meta            Meta            `json:"meta"`
}

>>> METADATA STRUCTURE <<<
type Meta struct {
        VersionId    string `json:"versionId"`
        LastUpdated  string `json:"lastUpdated"`
        Source       string `json:"source,omitempty"`
}

>>> IPS BUNDLE CONTAINER <<<
type IPSBundle struct {
        ResourceType string      `json:"resourceType"`
        ID           string      `json:"id"`
        Type         string      `json:"type"`
        Timestamp    string      `json:"timestamp"`
        Entry        []BundleEntry `json:"entry"`
        Meta         Meta        `json:"meta"`
}
```

Şekil 3.12 FHIR IPS Blokzincir veri modeli

Yaygınlaştırma sürecinin ilk aşamasında, zincirkodun (chaincode) kaynak kodundan dağıtıma uygun bir sıkıştırılmış paket (compressed package) oluşturma işlemi gerçekleştirilmiştir. Bu aşamada bağımlılıkların temizlenmesi amacıyla *"go mod tidy"* komutu çalıştırılmış, ardından *"peer lifecycle chaincode package"* komutu kullanılarak fhir-simple.tar.gz adlı zincirkod paketi oluşturulmuştur. Oluşturulan paket, eş düğüme (*peer node*) başarıyla kurulmuştur. *"peer lifecycle chaincode install"* komutu aracılığıyla zincirkod, eş düğümün yerel dosya sistemine yüklenmiş ve sistem tarafından benzersiz bir paket kimliği (package ID) üretilmiştir. Ardından, HospitalMSP organizasyonu

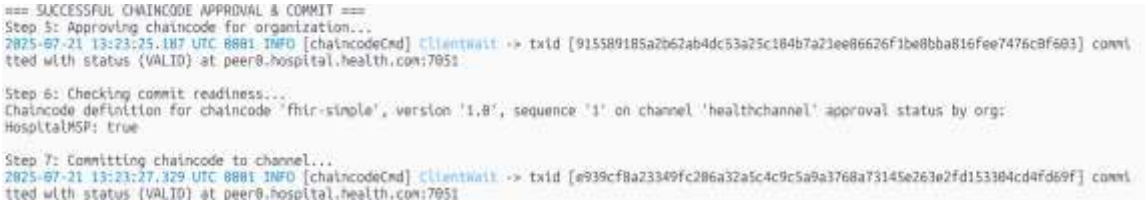
tarafından zincirkod onaylama işlemi gerçekleştirilmiştir. *"peer lifecycle chaincode app rove"* komutu kullanılarak organizasyonun zincirkodu onayladığı bilgi blokzincir defterine kaydedilmiştir. Yaygınlaştırmanın diğer bir adımı "commit" (onaylama ve etkinleştirme) aşamasıdır. Zincirkod, healthchannel kanalına başarıyla yüklenmiş ve peer lifecycle chaincode commit komutu aracılığıyla kanalda aktif hale getirilmiştir. Son olarak, yaygınlaştırmanın doğruluğu hasta verileri üzerinde gerçekleştirilen işlevsel testlerle sınanmıştır. Başarılı bir yaygınlaştırma süreci aşağıdaki kriterlerle doğrulanmıştır:

- Zincirkod durumu (Chaincode status) "DEPLOYED" olarak görünmektedir.
- Kanal durumu (Channel status) "healthchannel ACTIVE" şeklindedir.
- Hasta veri oluşturma (Patient data creation) ve sorgulama (query operations) işlemleri hatasız çalışmaktadır.
- Blokzincir ağı genel durumu (Blockchain network status) "FULLY FUNCTIONAL" olarak doğrulanmıştır.

Doğrulama aşamasında elde edilen JSON çıktısı, zincirkodun yaygınlaştırma detaylarını göstermektedir: Zincirkod "fhir-simple" adıyla, sürüm (version) "1.0" ve sıra numarası (sequence) 1 olacak şekilde kanala başarıyla tanımlanmıştır. Onaylama eklentisi (endorsement plugin) olarak "escc", doğrulama eklentisi (validation plugin) olarak ise "vscc" etkin durumdadır ve güvenlik politikaları çalışmaktadır. Validation parameter değeri, zincirkodun bütünlük kontrolü için kullanılmaktadır. Fonksiyonel test aşamasında, CreatePatient fonksiyonu çağrılarak "PAT001" kimlik numarasına sahip bir hasta oluşturulmuştur. Ardından GetPatient fonksiyonu ile hasta verileri sorgulanmış ve JSON formatında doğru biçimde döndürülmüştür. Test sonucu *{"id":"PAT001","name":"Ahmet Yılmaz","type":"Patient"}* şeklinde hasta bilgilerini doğru şekilde göstermektedir. (*Şekil 3.13*, *Şekil 3.14*, *Şekil 3.15*, *Şekil 3.16*)

Bu deployment süreci, FHIR tabanlı sağlık verilerinin blokzincir ortamında güvenli şekilde yönetilebileceğini pratik olarak kanıtlamaktadır. Sistemin operasyonel duruma geçmesi ile sağlık verilerinin blokzincir üzerinde işlenmeye hazır olduğu görülmektedir.

Şekil 3.13 Zincir kodu yaygınlaştırma süreci- 1



Şekil 3.14 Zincir kodu yaygınlaştırma süreci- 2

Şekil 3.15 Zincir kodu yaygınlaştırma) süreci- 3

Şekil 3.16 Zincir kodu yaygınlaştırma süreci- 4

3.12 Özel Veri Koleksiyonları (Private Data Collections) Gerçeklenmesi

3.12.1 Teorik altyapı ve gereksinim analizi

Bu çalışma kapsamında sağlık verilerinin blokzincir ortamında işlenmesi fikrindeki en kritik gereksinim, hasta mahremiyetinin korunması ve hassas kişisel verilerin (TC kimlik numarası, pasaport bilgileri gibi) sadece yetkili organizasyonlar tarafından erişilebilir olmasıdır (Zhang & Schmidt, 2018; Esposito et al., 2018). Geleneksel blokzincir sistemlerinde tüm veriler ağdaki tüm düğümler tarafından görülebilir durumda olduğundan, sağlık sistemleri alanında doğrudan uygulanmaları KVKK (Kişisel Verilerin Korunması Kanunu) ve GDPR (Genel Veri Koruma Tüzüğü) gibi veri koruma düzenlemeleriyle çelişki oluşturmaktadır (Voigt & Von dem Bussche, 2017; Kişisel Verilerin Korunması Kurumu, 2021). Bu ihtiyaca yönelik olarak, Hyperledger Fabric'in Private Data Collections (Özel Veri Koleksiyonları- PDC) özelliği kullanılarak, hassas sağlık verilerinin seçici açıklama modeli (selective disclosure model) ile yönetilmesi hedeflenmiştir (Hyperledger Foundation, 2024; Androulaki et al., 2018). PDC mekanizması, aynı kanal üzerindeki organizasyonlar arasında bile farklılaştırılmış erişim seviyeleri oluşturarak, sıfır-bilgi kanıtı (zero-knowledge proof) yaklaşımına benzer bir metodoloji ile veri gizliliği sağlamaktadır (Zyskind et al., 2015; Cavoukian, 2009). Bu yaklaşım ile çalışmamızda, blokzincirin şeffaflık özelliğini korurken, hassas verilerin sadece yetkili taraflarla paylaşılması mümkün olmakta ve böylece sağlık verisi yönetiminde "tasarımdan itibaren gizlilik" (privacy by design) prensibi uygulanmış olmaktadır.

3.12.2 PDC mimari tasarımı

PDC'nin temelini oluşturan koleksiyon politikaları (collection policy), Hyperledger Fabric'in izin tabanlı erişim kontrolü (permission-based access control) mekanizmasının bir bileşenidir. (Androulaki et al., 2018; Hyperledger Foundation, 2024). Bu politika tanımları, hangi organizasyonların hangi verilere erişebileceğini belirtir. Aynı zamanda verinin ne kadar süre saklanacağı ve dağıtım stratejileri de bu politikalarda belirlenir. Sağlık verilerinin hassasiyeti göz önüne alındığında, politikaların doğru tasarlanması

hasta mahremiyetinin korunması açısından oldukça önemlidir. Sistemde “hospitalPrivateCollection” isimli politika tanımlanmıştır. Amacı hasta kimlik bilgilerinin korunmasıdır. Bu politika, KVKK'nın "veri minimizasyonu" ve "amaca yönelik sınırlı olmak" ilkelerine uygun olarak tasarlanmış olup, rol bazlı erişim kontrolü (role-based access control) prensiplerini blokzincir ortamına uyarlamaktadır.

```
root@405735ffd51d:/opt/gopath/src/github.com/hyperledger/fabric/peer# cat collections_config.json
[
    {
        "name": "hospitalPrivateCollection",
        "policy": "OR('HospitalMSP.member')",
        "requiredPeerCount": 0,
        "maxPeerCount": 1,
        "blockToLive": 0,
        "memberOnlyRead": true,
        "memberOnlyWrite": true,
        "endorsementPolicy": {
            "signaturePolicy": "OR('HospitalMSP.member')"
        }
    }
]
```

Şekil 3.17 Politika (hospitalPrivateCollection) konfigürasyonu

Şekil 3.17 Politika (hospitalPrivateCollection) konfigürasyonu, en yüksek güvenlik seviyesi gereksinimlerini karşılamak üzere tasarlanmıştır. Policy'nin temel bileşenlerinden; ‘Erişim Kontrolü (Access Control): Policy’ parametresi "OR('HospitalMSP.member')" olarak tanımlanmış olup, sadece HospitalMSP organizasyon üyelerinin bu koleksiyona erişim yetkisine sahip olduğunu belirtmektedir. Bu yaklaşım, sağlık sistemlerinde bilme gereği (need-to-know) prensibini blokzincir ortamında uygulama imkanı sağlamak üzere oluşturulmuştur. (Ferraiolo et al., 2001). “Veri Dağıtım Stratejisi (Data Distribution Strategy): maxPeerCount: 1” parametresi, hassas verilerin maksimum 1 peer node'da fiziksel olarak saklanacağını garantilemek üzere yazılmıştır. Bu konfigürasyon, veri çoğaltma riskini azaltarak, KVKK'nın "veri güvenliği" maddesine uyumluluk sağlamaktadır. “requiredPeerCount: 0” ayarı ise, ağ erişilebilirliğini korumak amacıyla minimum peer gereksinimini esnekleştirmektedir. “Kalıcılık Yönetimi (Persistence Management): blockToLive: 0” değeri, hassas verinin süresiz olarak saklanacağını belirtmektedir. Sağlık verilerinin uzun vadeli arşivleme gereksinimleri ve tıbbi kayıt tutma yükümlülükleri göz önüne alındığında, bu konfigürasyon sağlık standartlarına uyumludur. “Okuma ve Yazma Kısıtlamaları: memberOnlyRead: true” ve “memberOnlyWrite: true” parametreleri hem okuma hem

yazma işlemlerinin sadece policy'de tanımlı organizasyon üyeleriyle sınırlandırıldığını belirtir. Bu "dual-restriction" yaklaşımı, veri bütünlüğünü ve gizliliğini aynı anda koruma altına almaktadır. “Onaylama Politikası (Endorsement Policy): endorsementPolicy” bölümündeki "OR('HospitalMSP.member')" tanımı, işlem onaylaması için HospitalMSP imzasının yeterli olduğunu belirtmektedir. Bu tek organizasyon onaylama modeli, kritik sağlık verilerinde hızlı karar alma ve kural koyma süreçlerini desteklerken, güvenlik gereksinimlerini de karşılamaktadır.

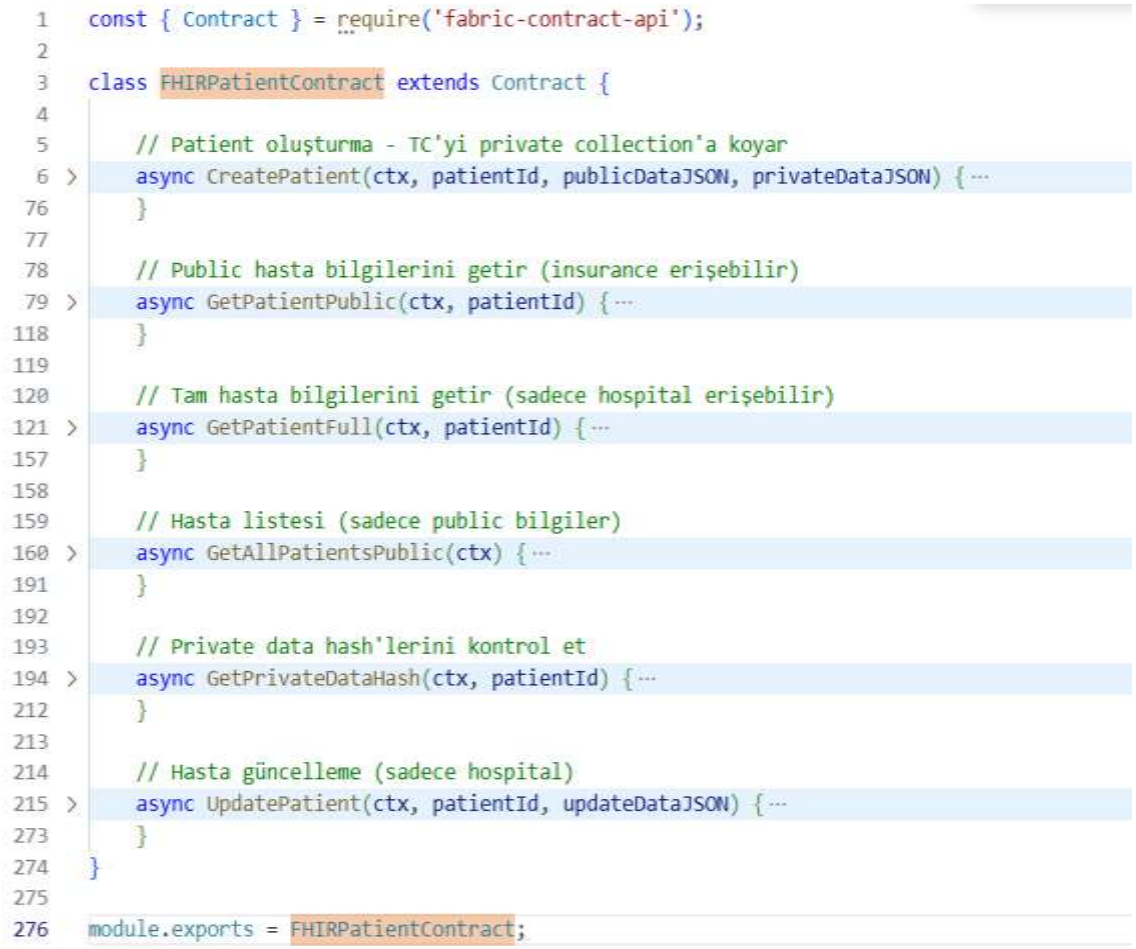
Çizelge 3.2 FHIR Hasta verilerinin ayrıştırma stratejisi

Veri Kategorisi	Depolama Konumu	Veri Türü	Açıklama	Erişim Yetkisi	KVKK Sınıflandırması
Demografik Bilgiler	World State (Public)	İsim (anonimleştirilmiş)	"Ahmet Can" → "A*** C***"	Tüm organizasyonlar	Genel kişisel veri
		Cinsiyet	"male", "female"	Tüm organizasyonlar	Genel kişisel veri
		Doğum tarihi	"1985-03-15" → "1985-03"	Tüm organizasyonlar	Genel kişisel veri
FHIR Metadata	World State (Public)	resourceType	"Patient"	Tüm organizasyonlar	Teknik metadata
		identifier	Sistem ID'si	Tüm organizasyonlar	Teknik veri
		managingOrganization	Sorumlu kuruluş referansı	Tüm organizasyonlar	Organizasyonel veri
Klinik Genel Bilgiler	World State (Public)	Alerji durumu (genel)	"Var/Yok" bilgisi	Tüm organizasyonlar	Genel sağlık verisi
		Genel tıbbi durum	Risk kategorisi	Tüm organizasyonlar	Genel sağlık verisi
Kimlik Bilgileri	hospitalPrivateCollection	TC kimlik numarası	"12345678901"	Sadece HospitalMSP	Hassas kişisel veri
		SSN	Sosyal güvenlik numarası	Sadece HospitalMSP	Hassas kişisel veri
		Passport numarası	Uluslararası kimlik	Sadece HospitalMSP	Hassas kişisel veri
Kişisel Detaylar	hospitalPrivateCollection	Anne kızlık soyadı	Güvenlik sorusu verisi	Sadece HospitalMSP	Hassas kişisel veri
		Acil durum iletişim	Yakın akraba bilgileri	Sadece HospitalMSP	Kişisel veri

Çizelge 3.2 FHIR Hasta verilerinin ayrıştırma stratejisi (devam)

Veri Kategorisi	Depolama Konumu	Veri Türü	Açıklama	Erişim Yetkisi	KVKK Sınıflandırması
Finansal Bilgiler	hospitalPrivateCollection	Sigorta numarası	SGK/Özel sigorta no	Sadece HospitalMSP	Finansal veri
		Ödeme bilgileri	Faturalama detayları	Sadece HospitalMSP	Finansal veri
Hassas Tıbbi Bilgiler	hospitalPrivateCollection	Detaylı alerji bilgileri	İlaç/besin alerjileri	Sadece HospitalMSP	Özel nitelikli kişisel veri
		Genetik predispositions	Kalıtsal hastalık riski	Sadece HospitalMSP	Özel nitelikli kişisel veri

Bu çalışmada geliştirilen FHIR IPS zincirkodu, Hyperledger Fabric Contract API v2.5.0 kullanılarak JavaScript (Node.js) programlama dili ile gerçeklenmiştir (implemente edilmiştir) (Hyperledger Foundation, 2024). Şekil 3.18 Chaincode sınıf yapısı ve temel fonksiyon kodları ekran görüntüsü ’nde görülen chaincode implementasyonu, Hyperledger Fabric'in Contract API'sini genişleterek, blokzincir ortamında sağlık verilerinin yönetimi için özelleştirilmiş fonksiyonlar sunmaktadır. Bu fonksiyonlar, hasta verilerinin oluşturulması, farklı yetkilendirme seviyelerinde sorgulanması ve özel verinin özet verisinin doğrulanması gibi kritik işlevleri kapsamaktadır. CreatePatient fonksiyonu, sistemin dual storage pattern'inin (ikili depolama modelinin) temelini oluşturmaktadır. (*Şekil 3.19 İkili depolama deseni (CreatePatient fonksiyonu*) Bu fonksiyon, gelen hasta verisini JSON formatında parse ettikten sonra, FHIR R4 standardına uygun şekilde açık ve özel olmak üzere iki farklı kategoride işlemektedir. Açık veriler (demografik bilgiler, genel tıbbi durum) World State'e kaydedilirken, hassas veriler (T.C. kimlik numarası, finansal bilgiler) hospitalPrivateCollection'a yönlendirilmektedir. Bu ayrım, KVKK'nın veri minimizasyonu ilkesini teknik olarak uygularken, blokzincirin şeffaflık özelliğini korumaktadır.



Şekil 3.18 Chaincode sınıf yapısı ve temel fonksiyon kodları ekran görüntüsü

Şekil 3.19 İkili depolama deseni (CreatePatient fonksiyonu)

GetPatientPublic fonksiyonu, gizlilik koruyan veri erişimi implementasyonunu gerçekleştirmektedir. Bu fonksiyon, World State'den hasta verilerini okuduktan sonra, anonimleştirme algoritmaları uygulayarak hassas kişisel tanımlayıcıları maskeler. İsim alanları "Ahmet Can" formatından "A*** C***" formatına dönüştürülürken, adres bilgilerinde sokak detayları çıkarılarak sadece şehir/ülke bilgisi korunmaktadır. Bu

yaklaşımı, demografik analiz gerekli olduğu durumlar için gerekli faydalanlamayı korurken, bireysel gizliliği korumaktadır.

GetPatientFull fonksiyonu, rol tabanlı erişim kontrolü mekanizmasının en önemli fonksiyonudur. Bu fonksiyon, çağıran organizasyonun MSP kimliğini ctx.GetClientIdentity().GetMSPID() metodu ile doğruladıktan sonra, sadece HospitalMSP organizasyonu üyelerine tam veri erişimi sağlamaktadır. Fonksiyon hem World State'deki public verileri hem de private collection'daki hassas verileri birleştirerek tam hasta kaydı oluşturur ve her erişimi denetim kaydı (audit trail) amaçlı blokzincire olay (event) olarak kaydeder. Bu yaklaşım, healthcare sistemlerinde kritik olan bilmesi gerekenler prensibini blokzincir ortamında uygulamaktadır.

GetPrivateDataHash fonksiyonu, zero-knowledge proof benzeri bir doğrulama mekanizması sağlamaktadır. Bu fonksiyon, özel verinin içeriğini açığa çıkarmadan varlığını SHA-256 hash'i ile kanıtlayabilmektedir. Hash değeri tüm organizasyonlar tarafından görülebilir olmasına rağmen, original data'ya reverse engineering (geri mühendislik) ile ulaşılması kriptografik olarak imkansızdır. Bu mekanizma, organizasyonlar arası doğrulama ve veri bütünlüğü kontrolü) için önemlidir.

En temel fonksiyonları yularıda verilen zincirkod implementasyonu, blokzincirin değiştiremezlik ve şeffaflık özelliklerini sağlık verilerinin gizliliği gereksinimleri ile dengelerken, FHIR standardının gerektirdiği ortak çalışabilirliği korumuş ve KVKK uyumluluğu sağlamıştır. Modüler yapısı sayesinde gelecekte ek FHIR kaynakları (Observation, Medication, Procedure gibi) ile yatayda genişleme ile ölçeklenebilirliğe imkân tanıyabilecektir.

4. BULGULAR VE SONUÇLAR

Bu bölümde, geliştirilen FHIR IPS tabanlı sağlık veri yönetimi blokzinciri sistemine ilişkin test ve değerlendirme sonuçları detaylı biçimde sunulmaktadır. Sistem, tasarlandığı mimari ve ihtiyaçlar çerçevesinde çeşitli işlevsel, güvenlik, gizlilik ve uyumluluk kriterlerine göre değerlendirilmiştir. Gerçekleştirilen testler, sistemin sağlık verilerinin güvenli, bütünlüklü ve birlikte çalışabilir şekilde yönetimine ne derece uygun olduğunu ölçmeyi amaçlamaktadır.

4.1 Test Planı ve Metodoloji

Önerilen sistem, hazırlanmış test senaryoları doğrultusunda test edilmiştir. Her bir senaryo, sağlık bilgi yönetimi sistemlerinin temel gereksinimlerini dikkate alarak oluşturulmuş, uygulanabilir işlevler ve teknik kontrol adımlarından oluşmaktadır. İlk aşamada fonksiyonel gereksinimlere yönelik senaryolar test edilmiştir. Chaincode dağıtımı, yaşam döngüsü yönetimi ve temel yazma ve okuma işlemleri gibi sistemin çekirdek işlevsellik testleri bu aşamada gerçekleştirilmiştir. Ayrıca eş zamanlı işlem talepleri ve yarış koşulları (race condition) gibi durumlar da değerlendirilerek sistemin güvenilirliği analiz edilmiştir. İkinci aşamada ise, sistem güvenlik ve gizliliğine dair test senaryoları oluşturulmuştur. Özel veri koleksiyonları (Private Data Collection) kullanımı, rol tabanlı erişim kontrolü ve sıfır bilgi kanıtlama (zero-knowledge proof) benzeri doğrulama mekanizmaları test edilerek sistemin hasta mahremiyetine duyarlılığı ve veri bütünlüğü değerlendirilmiştir. Bu kısımda test senaryoları oluşturulurken; HL7 FHIR R4 standardı ve IPS profili ile olan yapısal uyumluluk, ayrıca kişisel veri koruma düzenlemeleri (KVKK/GDPR) ile olan yasal uygunluk da göz önünde bulundurulmuştur.

4.2 Test Sonuçları

Test planına göre gerçekleştirilen test senaryoları ve elde edilen bulgular bu bölümde alt başlıklar altında detaylandırılmaktadır.

4.2.1 Fonksiyonel gereksinimler test sonuçları

Bu başlık altında, zincir kodu yaşam döngüsü, temel veri işlemleri ve eşzamanlı erişim senaryolarına yönelik testlerle ilişkin sonuçlar sunulmaktadır. İlgili test senaryoları:

Test Senaryosu 1: Zincir Kodu Yaşam Döngüsü Yönetimi Testleri: Zincir kodun kurulması, başlatılması ve güncellenmesi aşamalarının protokol uygunluğu ve işlevselliği bu testlerle doğrulanmıştır.

Testin Amacı ve Kapsamı: Bu test senaryosu, FHIR IPS zincir kodunun Hyperledger Fabric ağında yaşam döngüsü yönetimi süreçlerini kapsamlı bir şekilde değerlendirmek amacıyla oluşturulmuştur. Test, zincir kodun paketleme (packaging), kurulum (installation), onaylama (approval, commit ve activation) aşamalarının doğruluğunu ve güvenilirliğini analiz eder.

Test Metodolojisi: Hyperledger Fabric 2.5 lifecycle modelinde zincir kod yaygınlaştırma (chaincode deployment) süreci çok aşamalı bir protokol izler. Bu test, söz konusu protokolün her bir aşamasını doğrulamak ve sağlık alanında önemli olan FHIR IPS zincir kodun gerçek (production) ortamda güvenilir bir şekilde çalışabileceğini kanıtlar.

Test Uygulama Süreci: Hyperledger Fabric peer lifecycle komutları kullanılarak testler gerçekleştirilmiştir. İlk olarak, Go programlama dili ile geliştirilmiş FHIR IPS chaincode'u /opt/gopath/src/github.com/chaincode/fhir-ips dizininden paketlenmiş ve fhir-ips.tar.gz formatında yüklemeye hazır hale getirilmiştir. Ardından, bu paket peer0.hospital.health.com node'u üzerine kurulmuş ve sistem tarafından benzersiz bir package ID atanmıştır. Kurulum sonrası, HospitalMSP organizasyonu tarafından zincirkod onaylanmış (approve) ve commit'e hazır olma durumu kontrol edilerek tek organizasyonlu yapıda %100 hazırlık durumu sağlanmıştır. Son olarak, zincirkod healthchannel kanalına commit edilerek production ortamında invoke edilebilir duruma getirilmiştir. (FHIR IPS Zincirkod yaşam döngüsü süreci)

Şekil 4.1 FHIR IPS Zincirkod yaşam döngüsü süreci

Test Sonuçları ve Analizi: Tüm senaryo adımları, Çizelge 4.1'de sunulan "FHIR IPS Zincirkod yaşam döngüsü test adımları" içerisinde detaylı olarak gösterilmiştir. Test sürecinde elde edilen bulgular, FHIR IPS zincirkodunun Hyperledger Fabric 2.5 üzerinde başarılı bir şekilde dağıtılabildiğini ortaya koymaktadır. fhir-ips_1.0:…86 Package ID'si ile tanımlanan zincirkod, tüm yaşam döngüsü adımlarını hatasız bir şekilde tamamlamış ve 6c…41 (onay) ile dd…1a (commit) işlem kimlikleri üzerinden blokzincire değiştirilemez (immutable) şekilde kaydedilmiştir.

Çizelge 4.1 FHIR IPS Zincirkod yaşam döngüsü test adımları

Test No	Test Adımı	Komut/ İşlem	Beklenen Sonuç	Gerçek Sonuç	Durum
1.1	Chaincode paketinin oluşturulması	peer lifecycle chaincode package	Package dosyası oluşturulmalı	fhir-ips.tar.gz oluşturuldu. Chaincode dosyaları başarıyla paketlendi.	Başarılı
1.2	Chaincode yüklemenin gerçekleştirilmesi	peer lifecycle chaincode install	Package ID atanmalı	Package ID: fhir-ips_1.0:042a7bb71.... peer0.hospital.health.com üzerinde kurulum tamamlandı	Başarılı
1.3	Kurulumun Doğrulanması	peer lifecycle chaincode install	Yüklü chaincode listesinde görülmeli	Yüklü chaincode listesinde görüldü. fhir-ips_1.0 listelendi	Başarılı
1.4	Organizasyonun Onayı Alınması	peer lifecycle chaincode approveformyorg	HospitalMSP approval alınmalı	Transaction VALID (6c87df6b...). Organizasyon tarafından chaincode onaylandı	Başarılı
1.5	Commit Hazırlığı	peer lifecycle chaincode checkcommitreadiness	%100 readiness durumu	Tek organizasyon olduğu için tam readiness sağlandı	Başarılı

Çizelge 4.1 FHIR IPS Zincirkod yaşam döngüsü test adımları (devamı)

Test No	Test Adımı	Komut/ İşlem	Beklenen Sonuç	Gerçek Sonuç	Durum
1.6	Chaincode Commit	peer lifecycle chaincode commit	Channel'da aktif hale gelmeli	Transaction VALID (dd254285...). Chaincode healthchannel'da başarıyla commit edildi	Başarılı
1.7	Commit Doğrulama	peer lifecycle chaincode querycommitted	Committed listesinde görülmeli	Name: fhir-ips, Version: 1.0, Sequence: 1. Chaincode aktif durumda ve invoke edilmeye hazır	Başarılı

Elde edilen sonuçlar, blokzincir temelli bir sağlık ağı yapısı içerisinde chaincode yaşam döngüsü yönetiminin tam olarak işlevsel olduğunu ve FHIR IPS standardına uygun sağlık verisi yönetimi çözümlerinin Hyperledger Fabric platformu üzerinde güvenilir biçimde uygulanabildiğini kanıtlamaktadır. Chaincode, varsayılan güvenlik politikalarını sağlayan escc (endorsement system chaincode) ve vscc (validation system chaincode) eklentileri aracılığıyla üretim ortamında çalışmaya hazır (production-ready) hâle getirilmiştir.

Test Senaryosu 2: FHIR IPS Fonksiyon Testleri: FHIR IPS standardına uygun tasarlanan veri yapılarının ve ilgili işlevlerin beklenen operasyonları doğru bir şekilde yerine getirip getirmediği incelenmiştir.

Test Amacı ve Kapsamı: Bu test senaryosu, deploy edilmiş FHIR IPS chaincode'unun temel fonksiyonel gereksinimlerini karşılayıp karşılamadığını değerlendirmek amacıyla tasarlanmıştır. Test, hasta kayıt oluşturma (CreatePatient) ve hasta bilgisi sorgulama (GetPatient) operasyonlarının doğruluğunu, veri bütünlüğünü ve hata yönetim mekanizmalarını test etmektedir.

Test Metodolojisi: Sağlık Bilişimi domain ‘inde hasta kaydı için gerekli olan operasyonlardan Create ve Read fonksiyonları üzerinde odaklanılmıştır. Test metodolojisi, pozitif test case'leri (mevcut olan veri ile başarılı sorgulamalar) ve negatif test case'leri (mevcut olmayan veri ile başarısız sorgulama) içermektedir. Bu yaklaşım,

FHIR IPS uyumluluğunu da uygun olarak blokchain prensiplerinin bir arada test edilmesini sağlar.

Test Uygulama Süreci: Fonksiyonel test süreci üç aşamada gerçekleştirilmiştir. İlk aşamada, CreatePatient fonksiyonu kullanılarak ID "PATIENT001" ve name "Eray Ozcan" parametreleri ile yeni bir hasta kaydı olarak blokzincire yazılmıştır. Bu operasyon, zincir kodun invoke mekanizması aracılığıyla peer0.hospital.health.com node'u üzerinden orderer.health.com'a gönderilmiş ve distributed consensus sürecinden geçirilmiştir. İkinci aşamada, oluşturulan hasta kaydının doğruluğunu verify etmek amacıyla GetPatient fonksiyonu PATIENT001 ID'si ile sorgulanmıştır. Bu query operation, world state database'den ilgili kaydı okuyarak JSON formatında response döndürmektedir. Üçüncü aşamada ise, error handling ve boundary condition testleri için PATIENT999 gibi var olmayan bir ID ile GetPatient fonksiyonu çağırılmıştır.

Şekil 4.2 FHIR IPS Fonksiyon testleri

Test Sonuçları ve Analizi: Gerçekleştirilen test adımları, FHIR IPS chaincode'unun temel işlevsel gereksinimleri eksiksiz olarak karşıladığını ortaya koymaktadır. CreatePatient fonksiyonu, HTTP 200 durum kodu ile başarılı bir işlem tamamlanma mesajı vermiş ve bu durum, ilgili işlemin blokzincire sorunsuz biçimde kaydedildiğini (commit edildiğini) doğrulamıştır. GetPatient fonksiyonu geçerli bir kimlik numarası (ID) ile sorgulandığında, dönen JSON yanıt şu biçimdedir:

{"id":"PATIENT001","name":"Eray Ozcan","type":"Patient"}

Bu çıktı, HL7 FHIR standardındaki resource typing kurallarına uygun olarak "type": "Patient" alanını içermekte ve verinin doğru tanımlandığını göstermektedir. Özellikle

dikkat çeken önemli bir bulgu ise, geçersiz kimlik numarası ile yapılan sorguların hataya düşmeden kontrollü şekilde başarısız olmasıdır. PATIENT999 gibi sistemde bulunmayan bir hasta kimliği ile yapılan sorgu sonucunda chaincode boş bir yanıt döndürmüş ve bu durum, hata yönetim (exception handling) mekanizmasının doğru biçimde çalıştığını ve sistem kararlılığının (stability) korunduğunu ortaya koymuştur.

Çizelge 4.2 FHIR IPS fonksiyon testleri

Test Numarası	**Test Adımı**	**Komut/İşlem**	**Beklenen Sonuç**	**Gerçek Sonuç**	**Durum**
2.1	Hasta Oluşturma	CreatePatient	ID: PATIENT001 Name: Eray Ozcan	Transaction başarılı. Status:200 - Success	Başarılı
2.2	Hasta Sorgulama	GetPatient	ID: PATIENT001	JSON response. {"id":"PATIENT001","name":"Eray Ozcan","type":"Patient"}	Başarılı
2.3	Negatif Test	GetPatient	ID: PATIENT999	Empty/Error response. Boş satır – Cevap Yok	Başarılı
24	Veri Doğrulama	JSON yapısı	Patient object	FHIR compliant format. Valid JSON structure with type field	Başarılı

Test Senaryosu 3: Eşzamanlılık (Concurrency) ve Yarış Durumu (Race Condition) Testi: Sistemin yüksek hacimli eş zamanlı okuma/yazma işlemlerine maruz kaldığı durumlarda veri tutarlılığını koruma kabiliyeti ve potansiyel yarış durumu senaryolarına karşı dayanıklılığı test edilmiştir.

Testin Amacı ve Kapsamı: Bu test senaryosu, Hyperledger Fabric blokzincir ağı üzerinde eşzamanlı işlem yürütme kapasitesini ve yarış durumu (race condition) ortaya

çıktığında sistemin gösterdiği davranış kalıplarını sistematik biçimde analiz etmek amacıyla hazırlanmıştır. Özellikle sağlık alanı için kritik olan hasta kaydı güncelleme senaryolarında, eşzamanlı erişim denetimi, MVCC (Çok Sürümlü Eşzamanlılık Kontrolü) mekanizmasının etkinliği ve veri tutarlılığının korunması değerlendirilmektedir.

Test Metodolojisi: Bu testte kullanılan yöntem, aynı anahtar-değer çiftine eşzamanlı olarak yazma işlemi gerçekleştiren paralel işlem modeline dayanmaktadır. Arka planda çalışan işlemlerle, aynı hasta kimliğini (PATIENT003) hedefleyen ve farklı ad (name) değerleri ("User1" ila "User5") içeren 5 adet CreatePatient işlemi aynı anda orderer node'a gönderilmiştir. Bu yaklaşım, blokzincir konsensüs mekanizması ile World State veritabanının tutarlılık yönetimi yetkinliğini stres testi koşulları altında değerlendirmeye olanak sağlamaktadır.

Test Uygulama Süreci: Test uygulaması iki aşamalı olarak gerçekleştirilmiştir. İlk aşamada, temel durumu oluşturmak amacıyla PATIENT002 kimliğiyle bir kontrol kaydı oluşturulmuş ve işlem başarıyla tamamlanarak durum kodu 200 (Status: 200) doğrulanmıştır. İkinci aşamada, yarış durumu testi için hedef kimlik olarak PATIENT003 belirlenmiş ve Bash üzerinden arka plan işlemi notasyonu (&) kullanılarak beş eşzamanlı işlem başlatılmıştır. Bu işlemler orderer.health.com:7050 uç noktasına paralel olarak iletilmiş ve her bir işlemin tamamlanma süresi mikrosaniye düzeyinde izlenmiştir. İlk beşli işlem grubu yaklaşık 1 saniye içerisinde tamamlanırken, sonraki işlemlerde daha uzun gecikmeler gözlemlenmiştir. Bu zamanlama farkı, orderer bileşeninin yük dengeleme ve kuyruk yönetimi davranışlarını yansıtmaktadır.

Test Sonuçları ve Analizi: Uygulanan test adımları Çizelge 4.3 Eşzamanlılık ve yarış durumu test adımları'nda görülebilir. Hyperledger Fabric'in eşzamanlı işlem yönetiminde "son yazan kazanır" (last-write-wins) mantığını uyguladığını açıkça göstermektedir. Beş eşzamanlı işlemin tamamı HTTP 200 başarı durumu ile tamamlanmış, ancak world state içinde yalnızca kronolojik olarak en son kaydedilen değer ("User5") kalıcı hâle gelmiştir. Bu durum, blokzincirin gecikmeli tutarlılık (eventual consistency) modeli ve çakışma çözümleme stratejisini ortaya koymaktadır. Özellikle önemli olan bulgu ise; eşzamanlı

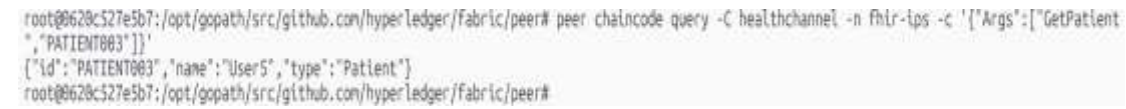
işlemler sırasında hiçbir veri bozulması, kısmi yazım (partial write) ya da tutarsız durum oluşumunun gözlemlenmemiş olmasıdır. GetPatient sorgusu, {"id":"PATIENT003","name":"User5","type":"Patient"} biçiminde geçerli bir JSON yanıtı döndürmüş, kontrol kaydı olan PATIENT002 ise {"id":"PATIENT002","name":"TestScenario3 User","type":"Patient"} olarak bozulmadan kalmıştır. Bu durum, Fabric'in izolasyon (isolation) özelliğini ve ACID uyumluluğunu sağlık gibi kritik uygulamalar için yeterli düzeyde sağladığını kanıtlamaktadır. (Şekil 4.3 Eşzamanlılık ve yarış durumu testi -1)

Performans açısından bakıldığında, ilk toplu işlemlerin (~1 saniye) tamamlanma süresi ile ardından gelen işlemlerin (~40 saniye) tamamlanma süresi arasındaki gecikme farkı, orderer düğümünün sıra yönetimi (queue management) ve uzlaşı (consensus) işleme yüküne bağlı olarak dinamik verim ayarlama yeteneğini göstermektedir. Bu özellik, üretim ortamlarındaki sağlık sistemlerinde beklenen işlem yükü için kapasite planlamasında dikkate alınmalıdır.

Çizelge 4.3 Eşzamanlılık ve yarış durumu test adımları

Test Adımı	Eşzamanlı İşlemler	Hedef Anahtar	Değerler	Tamamlanma Durumu	Zamanlama	Sonuç
Kontrol Testi	1 işlem	PATIENT002	TestScenario3 User	Durum: 200	~1 sn	Başarılı
Eşzamanlı Grup 1	5 işlem	PATIENT003	User1, User2, User3, User4, User5	Tümü Durum: 200	~1 sn	Başarılı
Eşzamanlı Grup 2	1 ek işlem	PATIENT003	User5 (tekrar)	Durum: 200	~40 sn	Başarılı
Son Durum Sorgusu	GetPatient	PATIENT003	Beklenen: Son yazılanın kalması	"User5"	Anında	Başarılı
Veri Bütünlüğü	Eşzamanlı erişim	Birden fazla anahtar	Bozulma yok	Tümü geçerli JSON	N/A	Başarılı

Şekil 4.3 Eşzamanlılık ve yarış durumu testi -1



Şekil 4.4 Eşzamanlılık ve yarış durumu testi -2

4.2.2 Güvenlik ve gizlilik test sonuçları

Bu bölümde, geliştirilen FHIR IPS tabanlı blok zinciri sisteminin güvenlik mimarisi ve hasta gizliliğini koruma kapasitesi kapsamlı bir şekilde değerlendirilmektedir. Test senaryoları, sistemin hassas sağlık verilerinin yetkisiz erişimlere karşı korunması, veri bütünlüğünün sağlanması ve yasal düzenlemelere (örneğin KVKK ve GDPR) uyum düzeyinin ölçülmesi amacıyla tasarlanmıştır. Sağlık bilişim sistemlerinde güvenlik ve gizlilik, yalnızca teknik bir gereklilik değil, aynı zamanda bireylerin temel hak ve özgürlüklerinin bir parçası olarak değerlendirilmelidir. Bu nedenle, geliştirilen sistemin hasta verilerinin mahremiyetini güvence altına alması ve yalnızca yetkilendirilmiş kurumlar arasında denetimli veri paylaşımına izin vermesi büyük önem taşımaktadır. Özellikle ulusal kimlik numarası, hastalık geçmişi, ilaç alerjileri gibi yüksek hassasiyete sahip bilgilerin işlenmesi, veri erişim kontrollerinin titizlikle uygulanmasını ve kayıt altına alınmasını zorunlu kılmaktadır.

Test Senaryosu 4: Private Data Collections Fonksiyonel Testleri- Hasta Oluşturma ve Veri Ayrıştırma Testi

Testin Amacı ve Kapsamı: Bu testin temel amacı, hasta verilerinin genel (public) ve özel (private) alanlara doğru şekilde ayrıştırılarak saklanıp saklanmadığını değerlendirmektir. Özellikle Türkiye Cumhuriyeti kimlik numarası gibi hassas verilerin yalnızca özel veri koleksiyonlarında korunup korunmadığı ve bu verilere yönelik erişim kontrollerinin güvenli bir şekilde işleyip işlemediği analiz edilmiştir.

Test Metodolojisi: Test kapsamında, CreatePatient, GetPatientPublic, GetPatientFull ve GetPrivateDataHash fonksiyonları sıralı test yöntemiyle çalıştırılmış ve her biri ayrı ayrı doğrulanmıştır. Bu yaklaşım sayesinde veri ayrıştırma işlemi ile özel verilerin erişilebilirliği değerlendirilmiştir.

Test Uygulama Süreci: Test senaryosunda "PATIENT001" kimliğiyle, gerçek hasta demografik bilgilerini ve hassas kimlik verilerini içeren test verisi kullanılmıştır. Test hasta bilgileri herkese açık (public) şekilde blokzincir üzerindeki world state durumuna kaydedilmiştir. Veriler arasında hastanın soyadı "Ozcan" ve adı "Eray" olarak belirtilmiştir. Ayrıca cinsiyet bilgisi "erkek" olarak tanımlanmıştır. Bu alanlar, FHIR R4 standardına uygun olarak name ve gender gibi temel demografik öğeleri temsil eder ve doğrudan sorgulanabilir niteliktedir. Özel veri olarak ise yalnızca yetkili organizasyonlar tarafından erişilebilecek şekilde, özel veri koleksiyonlarında saklanan hassas bilgiler yer almaktadır. Türkiye Cumhuriyeti kimlik numarası "12345678901" sistemin erişim kontrolü ve gizlilik ilkelerine uygun olarak blokzincir ağındaki diğer katılımcılardan gizlenmiş şekilde depolanmıştır. Bu veriler sadece yetkilendirilmiş eş düğümler (authorized peer node) tarafından erişilebilir durumdadır. *"CreatePatient"* fonksiyonu çağırıldığında, ikili depolama deseni (dual storage pattern) başarıyla uygulanmış ve hasta verisi iki farklı lokasyonda saklanmıştır: 1- Dünya Durum Veritabanı (World State Storage): FHIR R4 uyumlu Patient resource, tüm eş düğümlerde erişilebilir. 2- Özel Veri Deposu (Private Collection Storage): T.C. kimlik numarası ve SSN, sadece HospitalMSP yetkili peer'da erişilebilir

Test Sonucu ve Analiz: *Transaction response {"success":true,"message":"Patient created successfully","patientId":"PATIENT001"}* formatında dönerek, işlemin başarıyla tamamlandığını göstermiştir.

Şekil 4.5 Başarılı işlem logu (CreatePatient fonksiyonu)

Test Senaryosu 5: Private Data Collections Fonksiyonel Testleri- Veri Anonimleştirme Algoritma Testleri

Testin Amacı ve Kapsamı: Bu test senaryosunda, geliştirilen FHIR IPS blok zinciri sisteminin veri anonimleştirme algoritmasının etkinliği test edilmiştir. Test, hasta mahremiyetinin korunması ve KVKK gizlilik gereksinimlerinin karşılanması amacıyla tasarlanmış anonimleştirme mekanizmasının işlevselliğini doğrulamaktadır.

Test Uygulama Süreci: GetPatientPublic fonksiyonu, privacy-preserving data retrieval (gizlilik koruyan veri erişimi) implementasyonunu gerçekleştirmektedir. Bu fonksiyon, World State'den hasta verilerini okuduktan sonra, anonimleştirme algoritmaları uygulayarak hassas kişisel tanımlayıcıları maskeler. GetPatientPublic fonksiyonunun çalıştırılması sonucunda elde edilen JSON yapısı, FHIR R4 standardına uygun Patient kaynak formatında döndürülmüştür. Test sonuçlarında, hasta adı "Eray" orijinal değerinden "E***" şeklinde anonimleştirilmiş, hasta soyadı "Ozcan" orijinal değerinden "O***" şeklinde maskelenmiştir. Anonimleştirme algoritması, isim ve soyisim alanlarında ilk karakter koruma yaklaşımını benimseyerek, hasta kimliğinin tamamen gizlenmesi yerine demografik analizler için gerekli olan ilk harfin korunmasını sağlamıştır. Cinsiyet bilgisi "male" olarak açık şekilde korunmuş, doğum tarihi "1985-03-15" formatında hiçbir değişikliğe uğramadan sunulmuştur. Bu yaklaşım, demografik araştırmalar ve istatistiksel analizler için gerekli olan temel bilgilerin korunmasını sağlarken, kişisel tanımlama riskini minimize etmektedir. TC kimlik numarası gibi hassas

kişisel tanımlayıcı bilgiler, public sorgulamalarda hiçbir şekilde görüntülenmemiş, bu da özel veri koleksiyonlarının başarılı şekilde çalıştığını kanıtlamıştır.

Test Sonucu Analizi: Test süreci aynı zamanda sistemin erişim kontrolü mekanizmalarının etkinliğini de doğrulamıştır. HospitalMSP organizasyonu kimliği ile bağlı olunmasına rağmen, CLI ortamından yapılan sorgulama sadece anonimleştirilmiş verilere erişim sağlamıştır. Bu durum, sistemin peer düzeyinde uygulanan ek güvenlik katmanlarının varlığını ve MSP tabanlı yetkilendirme sisteminin çok katmanlı güvenlik yaklaşımını göstermektedir.

```
=== FHIR IPS Blockchain Test Environment ===
Current Configuration:
MSP ID: HospitalMSP
MSP Path: /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto-config/peerOrganizations/hospital.
health.com/users/Admin@hospital.health.com/msp
Channel: healthchannel
Chaincode: fhir-patient
Test Patient ID: PATIENT001
=== Testing Data Anonymization ===
root@fcb9c1df272b:/opt/gopath/src/github.com/hyperledger/fabric/peer# echo "=== GetPatientPublic Test
(Anonymization Proof) ==="
peer chaincode query -C healthchannel -n fhir-patient -c '{"Args":["GetPatientPublic","PATIENT001"]}'
=== GetPatientPublic Test (Anonymization Proof) ===
{"resourceType":"Patient","id":"PATIENT001","identifier":[{"use":"usual","system":"http://hospital.hea
lth.com/patient-id","value":"PATIENT001"}],"name":[{"given":["E***"],"family":"O***"}],"gender":"male"
,"birthDate":"1985-03-15","address":[],"telecom":[],"contact":[],"generalPractitioner":[],"managingOrg
anization":{"reference":"Organization/hospital-health-com"},"meta":{"lastUpdated":"2025-07-23T10:44:07
.895Z","versionId":"1"}}
root@fcb9c1df272b:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Şekil 4.6 Anonimleştirilmiş veri gösterimi

5. SONUÇ ve DEĞERLENDİRME

Bu tez kapsamında geliştirilen FHIR IPS tabanlı blokzinciri sistemi hem teknik işlevsellik hem de güvenlik-gizlilik gereksinimleri doğrultusunda hazırlanmış test senaryolarına tabi tutulmuştur. Gerçekleştirilen testler, sistemin Hyperledger Fabric altyapısı üzerinde uygulanabilirliğini, sağlık alanında işlevsel bir çözüm olabileceğini ve eşzamanlılık altındaki davranışlarını değerlendirmeye imkân sağlamıştır.

İlk olarak yürütülen zincir kodu yaşam döngüsü testleri, Hyperledger Fabric 2.5 sürümünün sunduğu modelin sağlık odaklı bir uygulama için işletilebileceğini ortaya koymuştur. Zincirkodun paketleme, kurulum, onaylama, uzlaşı ve sorgulama adımlarının tümü, beklenen çıktılar ile uyumlu sonuçlar vermiş; her işlem sistem tarafından geçerli durum ile doğrulanmıştır. Zincir kodun başarıyla kanal üzerinde kurulum yapılarak çağırılabilir hâle gelmesi, geliştirilmiş sistemin gerçek ortama taşınabilecek teknik olgunluk seviyesinde olduğunu da göstermiştir.

İkinci test senaryosunda, CreatePatient (Hasta kaydı oluşturma) ve GetPatient (Hasta Kaydı Elde Etme) fonksiyonları pozitif ve negatif test vakaları altında değerlendirilmiştir. Fonksiyonlar, FHIR R4 standardına uygun JSON veri yapılarıyla doğru yanıtlar döndürmüş; özellikle geçersiz hasta kimliği ile yapılan sorguların başarısız olarak işlenmesi, zincir kod içindeki hata yönetimi mekanizmalarının sağlıklı çalıştığını göstermiştir. Bu durum, yalnızca başarılı işlemlerin değil, başarısızlık senaryolarının da kontrollü biçimde ele alındığını göstermektedir.

Üçüncü test kapsamında gerçekleştirilen eşzamanlılık ve yarış durumu testleri, aynı hasta kimliğine eşzamanlı olarak gönderilen beş farklı işlem sonucunda yalnızca son yazımın kalıcı hâle geldiğini göstermiştir. Bu davranış, Hyperledger Fabric'in MVCC (Multi-Version Concurrency Control) mekanizmasının öngördüğü "last-write-wins" (son yazılanın kazanması) modeline tam uyumlu işletildiğini ve sistemin eşzamanlı işlem yükü altında bile veri bütünlüğünü bozmadan çalışabildiğini göstermiştir. Her bir işlem HTTP 200 yanıtı ile başarılı olarak tamamlanmış, ancak world state üzerinde yalnızca en son işlem sonucu yer almıştır. Bu durum, Fabric'in ACID özelliklerini destekleyen yapısının

sağlık sektörü gibi yüksek bütünlük gerektiren alanlarda etkili biçimde çalışabileceğini göstermektedir.

Yukarıda bahsedilen yalnızca teknik işlevsellik sonuçlarına göre değil, aynı zamanda veri güvenliği ve hasta mahremiyeti açısından da yapılan testler, sistemin güvenilir bir sağlık blokzinciri çözümü sunduğunu ortaya koymuştur. Gerçekleştirilen diğer testler, hassas verilerin korunması, erişim kontrolünün uygulanması ve yasal düzenlemelere uyum gibi temel gereklilikler doğrultusunda başarılı sonuçlar vermiştir. KVKK ve GDPR gibi mevzuatlar çerçevesinde, bireylerin mahremiyet haklarına saygı gösterilerek veri erişim ve paylaşım mekanizmaları uygulanabilmektedir. Veri ayrıştırma testleri, hasta bilgilerini genel (public) ve özel (private) alanlara ayırarak veri saklamanın başarıyla gerçekleştirilebildiğini göstermiştir. World State üzerinde saklanan ad, soyad, cinsiyet ve doğum tarihi gibi demografik bilgiler tüm ağ katılımcılarına açıkken, Türkiye Cumhuriyeti kimlik numarası gibi yüksek hassasiyete sahip bilgiler yalnızca yetkili organizasyonların eş düğüm sunucularında ve özel veri koleksiyonlarında tutulmuştur. Böylece hem erişilebilirlik hem de gizlilik sağlanmıştır.

Anonimleştirme testlerinde kullanılan maskeleme algoritmaları, hasta adı ve soyadında yalnızca ilk harfin görünür kılındığı, geri kalan karakterlerin yıldız (*) ile gizlendiği bir modelle uygulanmıştır. Bu sayede kişisel tanımlayıcı bilgilere erişim sınırlandırılırken, demografik analizler için gerekli bilgi korunmuştur. Doğum tarihi ve cinsiyet gibi alanların değişmeden sunulması, sistemin yalnızca tanımlayıcı alanları anonimleştirdiğini ve FHIR uyumlu veri bütünlüğünü koruduğunu ortaya koymuştur. Erişim kontrol testlerinde ise, Membership Service Provider (MSP) tabanlı yetkilendirme mekanizmalarının işlevselliği doğrulanmıştır. Yetkisiz bir MSP kimliği ile GetPatientFull fonksiyonunun çalıştırılmaya çalışılması sonucunda sistem, açık bir hata mesajı ile erişimi reddetmiş ve yalnızca yetkili organizasyonlar tarafından tam veri erişimine izin verildiğini göstermiştir. Bu çok katmanlı güvenlik yapısı, yalnızca kimlik doğrulamasına değil, organizasyona göre değişen politika bazlı yetkilendirmenin de mümkün olarak tasarlandığını göstermektedir.

Genel olarak değerlendirildiğinde, geliştirilen FHIR IPS tabanlı blokzinciri sistemi, yalnızca işlevsel olarak değil, aynı zamanda güvenlik, gizlilik ve yasal uygunluk açısından da başarılı bir çözüm ortaya koymuştur. Tez çalışmamızda, sağlık verilerinin güvenli şekilde işlenmesi, saklanması ve paylaşılması için blokzincir teknolojisinin sunduğu temel avantajlar detaylı şekilde değerlendirilmiştir. Ayrıca HL7 FHIR standardına dayalı veri modellemesi, sistemin sağlık sektöründeki teknolojik altyapılarla entegrasyon potansiyelini ve ortak çalışabilirliğe uygun tasarlandığını göstermektedir. Sonuç olarak bu çalışma, blokzincirin yalnızca merkeziyetsiz bir veri mimarisi sunmakla kalmadığını, birçok alanda ihtiyaca yönelik bir çözüm mimarisi de oluşturabileceğini somut biçimde ortaya koymuştur.

KAYNAKLAR

Agbo, C. C., Mahmoud, Q. H., ve Eklund, J. M. 2019. Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... ve Yellick, J. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Proceedings of the Thirteenth EuroSys Conference, 1-15.

Azaria, A., Ekblaw, A., Vieira, T., ve Lippman, A. 2016. MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD), 25-30.

Bahga, A. ve Madisetti, V. K. (2020). Blockchain Applications: A Hands-On Approach. VPT.

Christidis, K. ve Devetsikiotis, M. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

Conti, M., Kumar, S., Lal, C. ve Ruj, S. 2018. A survey on security and privacy issues of blockchain technology. IEEE Communications Surveys & Tutorials, 21(2), 1165-1190.

Crosby, M., Pattanayak, P., Verma, S. ve Kalyanaraman, V. 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

Dagher, G. G., Mohler, J., Milojkovic, M. ve Marella, P. B. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. ve Wang, F. 2017. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annual Symposium Proceedings, 2017, 650-659.

Engelhardt, M. A. 2017. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10), 22-34.

Esposito, C., De Santis, A., Tortora, G., Chang, H. ve Choo, K. K. R. 2018. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing, 5(1), 31-37.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42(7), 130.

HL7 International. 2022. International Patient Summary (IPS) Implementation Guide: STU 1.1.0. HL7. Erişim adresi: https://hl7.org/fhir/uv/ips/

Hyperledger Foundation. 2024. Hyperledger Fabric Documentation. Erişim adresi: https://hyperledger-fabric.readthedocs.io/en/latest/

Iroju, O. G., Soriyan, A., Gambo, I. ve Olaleke, J. (2018). Interoperability in healthcare: Benefits, challenges and resolutions. International Journal of Innovation and Applied Studies, 3(1), 262–270.

ISO. (2016). ISO/TS 18308: Health Informatics – Requirements for an Electronic Health Record Architecture. International Organization for Standardization.

Kuo, T. T., Kim, H. E. ve Ohno-Machado, L. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

Mettler, M. 2016. Blockchain technology in healthcare: The revolution starts here. IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Swan, M. 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, 1-xx, (şehir yoksa belirtmeyebilirsiniz).

Tapscott, D. ve Tapscott, A. 2016. Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.

Yue, X., Wang, H., Jin, D., Li, M. ve Jiang, W. 2016. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.

Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. First Monday, 2(9).

Zyskind, G., Nathan, O. ve Pentland, A. 2015. Decentralizing privacy: Using blockchain to protect personal data. IEEE Security and Privacy Workshops, 180-184.