**GÜFBED/*GUSTIJ* (2020) 10 (1): 35-42** **Gümüşhane Üniversitesi Fen Bilimleri Enstitüsü Dergisi**
DOI: 10.17714/gumusfenbil.437775 Araştırma Makalesi / *Research Article*

# Blok Zinciri Mimarisi ile Elektronik Tıp Kayıtlarının Modellenmesi Üzerine Bir Araştırma

*A Survey on Modeling of Electronic Medical Records with Blockchain Architecture*

**Ömer KASIM***

*Kütahya Dumlupınar Üniversitesi, Simav Teknoloji Fakültesi Elektrik Elektronik Mühendisliği, Kütahya*

• Geliş tarihi / *Received*: 27.06.2018 • Düzeltilerek geliş tarihi / *Received in revised form*: 25.09.2019 • Kabul tarihi / *Accepted*: 3.10.2019

**Öz**

Günümüzde veriler, bilgisayar destekli günlük hayat faaliyetlerinin neredeyse tamamını kapsamaktadır. Bu durum kişiye ait verilerin oldukça artmasına neden olmaktadır. Kişisel verilerdeki müthiş artış, depolama ve yönetim süreçlerinde bulut ortamını gerekli kılmaktadır Kişinin sağlıkla ilgili hassas verilerinin bulut ortamında saklanması ve korunması kritik öneme sahiptir. Bu problemin çözümünde farklı yaklaşımlar olsa da Blok Zinciri mimarisi gizliliği, güvenliği ve ölçeklenebilirliği kapsayan bir çözüm sunmaktadır. İzinli ve izinsiz olmak üzere iki farklı şekilde tasarlanabilen Blok Zinciri mimarisinde, veriler bloklar halinde saklanmaktadır. Çalışmada yapılan araştırma sonucu verilerin blok zinciri içerisinde organize edilmesi ile elektronik tıbbi kayıtların güvenli bir şekilde oluşturulması, erişilmesi ve paylaşılmasının mümkün olduğu tespit edilmiştir.

**Anahtar kelimeler:** Blok Zinciri, Elektronik Tıp Kayıtları, İzinli Blok Zinciri Mimarisi, İzinsiz Blok Zinciri Mimarisi, Veri Paylaşımı

***Abstract***

*Nowadays, the data cover almost all of the computer-assisted daily life activities. This leads to a significant increase in the number of data per person. The tremendous increase in personal data requires a cloud environment during storage and management processes. Preservation and protection of the sensitive health-related data of the person in the cloud environment is critical. Although there are different approaches to solve this problem, Blockchain architecture offers a solution that covers privacy, security and scalability. In this architecture, which can be designed in two different ways, with authorized and without permission, the data are stored in blocks. As a result of this study, it is possible to securely create, access and share electronic medical records by organizing data within the block chain.*

***Keywords**: Blockchain, Electronic Medical Records, Authorized Blockchain Architecture, Without Permission Blockchain Architecture, Data Sharing*

* Ömer KASIM; omer.kasim@dpu.edu.tr, Tel: (0542) 716 85 48, orcid.org/0000-0003-4021-5412

## 1. Giriş

Sağlık Bilgisi Sitemi (SBS) sürecindeki bir model olan Elektronik Tıp Kayıtları (ETK), sağlık hizmetleri sürecinde önemli yer tutmaktadır (Hauxe,2006). Bu bilgiler kullanılarak sağlık hizmeti veren kurumlar, sigorta şirketleri, eczaneler, araştırmacılar ve hasta aileleri arasında bağlantı kurulmaktadır (Steward,2005). Bu bağlantı içerisinde hastaya ait verilerin dağıtımı ve paylaşımı süreci yer almaktadır. Hastaya ait veriler, teşhis ve tedavi süreçlerini içermektedir. Bu süreçte yer alan veriler, veritabanı içerisinde hassas veri olarak saklanmaktadır. Verilerin hassas olması ve kişisel içeriğin paylaşılmaması açısından bakıldığında hastanın tıbbi geçmişini güncel tutmak noktasında önemli bazı sorunlar bulunmaktadır. Bu sorunlar; birden fazla birim arasında oluşacak olan veri saklama, veri paylaşma, veriye erişimin kontrolü ve veriye erişim aşamasındaki onay süreçleri olarak sıralanmaktadır (Mandl vd., 2001). Bu kapsamda oluşacak zincire bakıldığında hastanın tedavi sürecini zorlaştırıcı bir süreç karşımıza çıkmaktadır. Kanser ve HIV gibi ciddi bir tıbbi rahatsızlığı olan bir hastanın hikâyesinin oluşumundaki temel faktörler olan tedavi süreci ve tedavi sonrasındaki iyileştirme ile izlemenin her aşamasına ait verilerin korunması gerekmektedir. Hastaya ait tüm verilerin erişilebilir bir alan içerisinde tutulmasıyla hastanın daha önceki kayıtları sayesinde tedavi süreci daha net planlanabilecektir. Özellikle tedavi süreci gereken hastalıklarda uygulanan ilaç tedavisi, gözlem süreci ve tetkiklerin sonuçlarının takibi tedavinin yönlendirilmesi noktasında önem arz etmektedir (Azaria vd, 2016).

ETK sadece tek bir sağlık kuruluşu içerisinde yer almayabilmektedir. Bir hasta görüş alışverişi için birden fazla sağlık kurumunu ziyaret edebilmektedir. Ayrıca hastaneler arası transfer süreci de olabilmektedir. Böyle bir durumda hastaya ya da hastanın belirlediği kişilere sağlık bilgisi hakkında bilgi edinme hakkı verilmesi gerekmektedir (The Office of the Nat. Coordinator for Health Information Technology, 2018). Diğer taraftan hastalığı konusunda kişi, kurallar ve limitler belirleyebilmektedir. Bir hastanın klinik verilerinin araştırma amacıyla paylaşılması noktasında ya da bu bilgilerin bir hastaneden diğerine aktarması gerektiği durumlarda bazı yetkilendirmeler yapılmaktadır. Bu yetkilendirmelerin kapsamını, hangi tür verilerin paylaşılacağını, alıcıyla ilgili bilgileri ve süreyi belirten bir süreç oluşturmaktadır (Tang vd, 2006). Ancak yetkiye sahip kişiler veya birimler verilere erişim sağlayabilmektedir. Hastanın başka bir şehre, bölgeye veya ülkeye gitmesi durumunda sürecin koordinasyonu son derece zorlayıcı olmaktadır. Çünkü bir sonraki bakım alınacak bakıcı veya hastaneyi önceden bilmeme durumu söz konusudur. Verilerin aktarılması noktasında elektronik kayıtların yanı sıra posta ile gönderilen verilerin olması durumunda hassas bilgilere izin verilmesi, verilerin aktarılması süreci zaman alıcı olduğu gerçeğini değiştirmemektedir. Hastanın sağlık kayıtlarının transit geçişi sırasında güvenlik riskine yol açabileceğinden hastaların verilerini internet üzerinden e-posta yoluyla gönderilmesi genellikle tercih edilmemektedir. Günümüz veri kayıt sistemi içerisinde mobil cihazların da sürece dahil olması bu durumu tetiklemektedir. Bu cihazlar verileri anlık kullanarak istatistiksel sonuçlar üretmektedir (He vd., 2016).

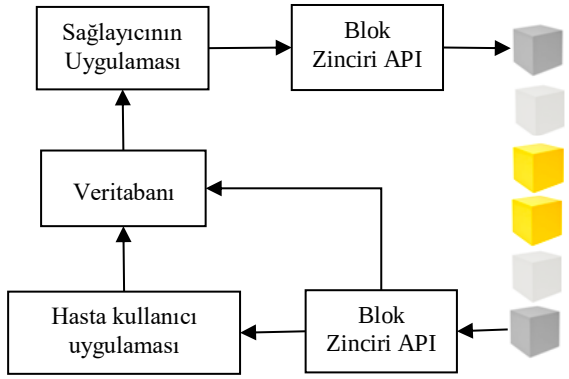
Araştırma amacı için kullanımı gereken tıbbi kayıtlar üzerinde veri toplama yapılacaksa verilerin anonim hale getirilmesi gerekmektedir. Anonim hale gelmeyen veriler üzerinde araştırma yapılması için hastanın kendisinden özel izin alınması gerekmektedir. Lokal olarak anonimleştirilmiş bilgiler üzerinden kullanılan tıbbi verilerin hastanın kimliğini açık etmesi mahremiyetin ihlaline neden olmaktadır. Bu süreçte güvenirliği sağlamak amacıyla anonim hale getirilen veriler saklanırken şifrelenmektedir (Poh vd., 2017). Hastanın verilerini depolamak ve yönetmek amacıyla oluşturulan merkezi bir veri yönetim sistemine güvenmek ve kontrol politikalarına erişimin gerektirdiği kuralların belirlenmesi önem arz etmektedir. Bunun sebebi sistemde oluşabilecek güvenlik problemi belki de tüm ülkenin sağlık verileri açısından bir darboğaza sürüklenmek anlamına gelmektedir. Güvenlik açıklarının hastaya ait hassas verilerin şifrelenmesi, bu verilerin erişim isteği anında tamamen güvenilir bir erişim sürecinin olmasına ihtiyaç bulunmaktadır. Bu yazılımın içerisinde tüm hasta kayıtları olacağından büyük miktarlarda belleğin yönetimi gerekmektedir. Bu şekilde yapılan kaynak yönetimi hastane ortamındaki veri merkezleri için oldukça büyük olduğundan dolayı bulut ortamının kullanılması gerekli olmaktadır. Bulut ortamında büyük verinin analizi ve verilerin güvenliği sürece dahil olmaktadır (Kuo, 2011). Bu süreçlerin bulut sistemi içerisinde takibi ve yönetilmesi amacıyla oluşturulacak Blok Zinciri yapısı hasta elektronik sağlık kaydının veri formunun güvenli, verimli ve doğru bir şekilde paylaşılması sağlanabilmektedir (Tschorsch vd, 2016; Zhang vd., 2016).

## 2. Blok Zinciri Mimarisinin Tasarımı

Blok Zinciri, finans sektöründe kullanılan eşler arası dağıtılmış blok teknolojisi üzerine inşa edilmiştir. Bir kullanıcının kimliğinin bir ağ içinde nasıl tanımlandığına bağlı olarak izin verilen ve izinsiz blok zinciri sistemleri olarak iki farklı türde tasarlanabilmektedir (Lee vd., 2018). İzinsiz bir sistem tasarımında katılımcıların kimliğinin sahte veya anonim olması önem arz etmemektedir. Bu tasarımda her kullanıcı Blok Zinciri mimarisine yeni bir blok ekleyebilmektedir. Diğer taraftan izin verilen bir blok zincir tasarımında ise bir kullanıcının kimliği, bir kimlik sağlayıcı tarafından kontrol edilmektedir. Bu tasarımda kimlik sağlayıcısının rolü kritik öneme sahiptir. Bu sağlayıcı, ağ içinde erişim kontrolünü ve kullanıcının uzlaşmaya katılma haklarını koruma görevini üstlenmektedir. Ayrıca yeni bir bloğu onaylamak için güvenilir olması zorunluluğu bulunmaktadır (Sara vd., 2018).

### *2.1. İzinsiz Blok Zinciri Tasarımı*

İzinsiz tasarıma ait Blok Zinciri mimarisi Şekil 1'de gösterilmiştir (Şekil 1). Mimaride uygulama sağlayıcı hizmeti ile veritabanı hizmeti hasta kullanıcı uygulamasına bağlıdır. Üretilen her bir veri sağlayıcı uygulaması üzerinden bir API aracılığıyla Blok Zinciri olarak eklenmektedir. Eklenen bu blok yine API üzerinden hasta kullanıcı uygulamasına veri sağlayarak döngüyü oluşturmaktadır.




**Şekil 1.**İzinsiz blok zinciri mimarisi

İzinsiz Blok Zinciri tasarımında herhangi bir kullanıcı, platformda isteğe bağlı bir algoritma ile karmaşıklık kodunu oluşturabilmekte ve çalıştırabilmektedir. Bu süreç İzinsiz programlanabilir bir tasarım uygulamasıdır. Uygulamalar sanal makine üzerinde koşturulduğundan ana sistemden bağımsız süreç yönetilmektedir. İzinsiz Blok Zinciri Sanal Makine üzerinde iki farklı türde "hesap" oluşturulabilmektedir. Bu hesaplardan ilki Harici olarak sahip olunan hesaptır (Cruz vd., 2018). Bu hesap, bir kullanıcının özel anahtarı tarafından kontrol edilen yapıdadır. Diğer hesap ise Sözleşme Hesabı'dır. Sözleşme hesabında İzinsiz Blok Zinciri yürütme ortamında bulunan ve sözleşme koduyla kontrol edilen tekil bir aracı olarak görülebilen ikinci tür hesaptır. Bu tür hesaplara akıllı sözleşme ismi verilmektedir. Akıllı sözleşme, kişisel durum geçişi işlevlerini kodlamak için kullanılmaktadır. Bu sözleşme ile kullanıcıların sistem mantığı koda dönüştürülerek farklı işlevlere sahip sistemler oluşturması sağlanmaktadır.

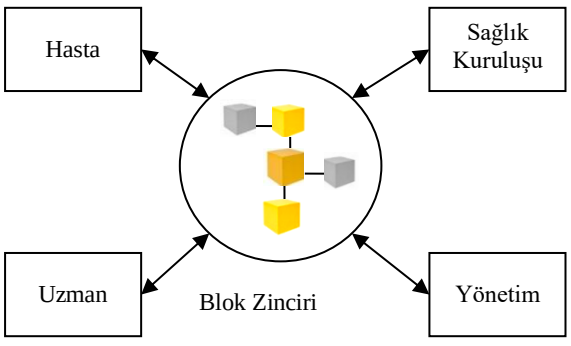
İzinsiz Blok Zinciri'nde kod çalıştırma süreci, ödemeli olarak tasarlanmıştır. İşlem ücreti, sonsuz döngüleri veya diğer hesaplama işlemlerini önleme noktasında kod yürütme esnasında hesaplamalı adım sayısını sınırlamak amacıyla tasarlanmıştır. Kullanıcılar, işlemin yürütülmesi için ödenecek jetonları elde etmek için bir fikir birliği sürecine katılması gerekmektedir. Bu mimaride bir Proof of Work (PoW) mekanizması kullanılarak uzlaşma elde edilir (Mengelkamp vd., 2018). PoW, madencilik esasına dayanmaktadır. Madencilik sürecinde algoritmaya ait olmayan girdi bulmak önem arz etmektedir. Her bir farklı girdi yeni bir geçerli bloğun elde edilen farklı gereksinimleri karşılamaktadır. Bu gereksinimler, "nonce" bulma işlemi için zorluk eşiğini belirlemektedir. "Nonce" bir hesabın işlem sayısını ifade etmektedir (Chang vd., 2016). İşlem sayısının takip edilmesi enerji tüketimini doğrudan etkilediği için önemli bir parametredir. Mevcut PoW blok işlemleri, blok zinciri'nin güvenliğini önemli ölçüde etkilemeden saniyede 60'tan fazla işlem üretememektedir. Bu iki bulgu, PoW'nun sistem ölçeklenebilirliğini ve genel üretkenliğini olumsuz etkileyebileceğini göstermektedir. Bu sınır değerler siber saldırı olması durumunda sistemin %51'inin ele geçirilmesini önlemeye yönelik yapılan bir tasarımdır (Karaarslan vd., 2017).

Proof of Stake (PoS), Proof-of-Burn (PoB) ve sanal madencilik mekanizmaları son zamanlarda PoW'a alternatif olarak önerilmektedir (Pavel vd., 2018). Katılımcıların varlıklarını hesaplama kaynakları için değiştirerek benimsemek yerine sanal madencilikte katılımcılar, kayıtlarını doğrudan zincire yeni bir blok ekleyebilecekleri şekilde değiştirebilmektedir. Örneğin, PoS'de, yeni bir blok oluşturacak bir katılımcının seçimi, katılımcı tarafından sahip olunan jeton miktarına

dayanmakta ve PoB cinsinden verilmektedir. Bununla birlikte, sanal madenciliğin istikrarı için açık bir problem olmaya devam etmektedir.

### *2.2. İzinli Blok Zinciri Tasarımı*

İzinli blok zinciri mimarisinde tüm blok yapısı merkezi bir noktada dağıtık olarak tutulmaktadır. Şekil 2'de gösterilen sistem üzerinde kullanıcı yetkisine sahip 4 farklı kullanıcı kendilerine verilen rollere göre sınırlamalar getirilerek sisteme erişim sağlamaktadır (Şekil 2). Kullanıcı rolleri, ETK uygulamasında Hasta, Uzman, Yönetim ve Sağlık Kuruluşu'dur. Bu rollere göre izinli bir Blok Zinciri tasarımında kullanıcıların kimlik sunucusu kullanıcı kimliklerini açığa vurmadıkça gizlilik sağlanmaktadır. Ayrıca bu tasarımda uzlaşma yönetimine katılım önceden tanımlanmış bir kullanıcı grubuyla sınırlıdır. Bu durum bir uzlaşma mekanizması olarak bir durum makinesi çoğaltma algoritmasını (PBFT19) kullanma olasılığını açmaktadır (Lemieux, 2017). İzinli Blok Zinciri, izinli ve açık kaynaklı bir Blok Zinciri uygulamasıdır. İzinli Blok Zinciri, PBFT de dâhil olmak üzere farklı uzlaşma mekanizmalarını barındıran modüler bir mimariye sahiptir. İzinli blok zinciri hizmetleri üç kategoride gruplandırılmaktadır. Bunlar üyelik hizmetleri, blok zinciri hizmetleri ve zincir kod hizmetleridir.




**Şekil 2.**İzinli blok zinciri mimarisi

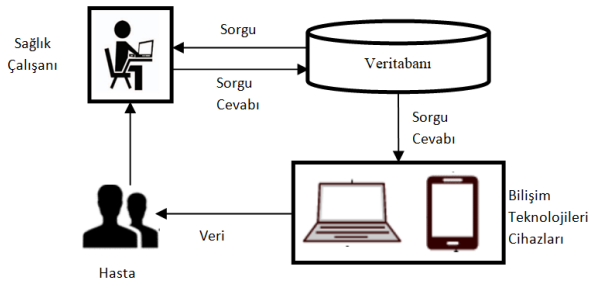
Üyelik hizmetleri ağdaki kimlik bilgilerini ve kişisel gizliliği yönetmek amacıyla kullanılmaktadır. Bir kullanıcıya ağdaki kayıtlı kullanıcılarını tanımlamak için Kayıt sertifikası (ECert) verilmektedir. Bu sertifika için kullanılacak bir kullanıcı adı ve şifre atanmaktadır. Bağlantı yönetimini sağlama noktasında her bir işlem için aynı ECert ile ilişkilendirilmiş farklı İşlem sertifikalarını (TCert) kullanmak mümkündür (Liang vd., 2017). Bu iki sertifika arasında bir haritalama bulunmaktadır. Bu süreç sadece üyelik hizmetiyle bilinmektedir. Blok Zinciri hizmetleri dağıtılmış defterleri Http/2 üzerinde oluşturulmuş eşler arası bir protokolle yönetilmektedir. İzinli Blok Zinciri yapısında akıllı sözleşmeler, zinciri koduyla uygulanmaktadır. Bu durum zincir kod hizmetleri doğrulama düğümlerinde akıllı sözleşmeler yürütmek için güvenli bir yol sağlamaktadır.

İzinli Blok Zinciri yapısında akıllı sözleşmeler, kuruluşun kurallardan oluşan zincir kodu ile uygulanmaktadır. Zincir kodunun mantığı, işlemlerin nasıl yürütüleceğini ve belirlenen kuralların nasıl değişeceğini tanımlayan bir kurallar bütününden oluşmaktadır. Durum bilgileri bayt dizileri olan anahtar ve değerler biçiminde depolayan bir veritabanında tutulmaktadır. İzinli Blok Zinciri, bir bloğa eklenirken ilgili kuruluşun verimli bir kriptolojik karmasını ekleyerek blok zincirini yönetmektedir. Bu olgu düğümün geçici olarak devre dışı kalması durumunda düğümdeki depolanmış verilerin miktarının en aza indirilmesiyle etkili bir senkronizasyona izin vermektedir.

İzinli blok zincir'e erişime sahip olan bir uzman, hasta izinleri, farklı bir ortama transfer edilen veriler veya araştırma amacıyla paylaşılan veriler noktalarında ağa müdahale ederek değişikliklere sebep olmaktadır. Bu durum ağdaki tüm kullanıcılara iletilmesi ve ağın kendini güncellemesi gerekmektedir. Sadece bir tek güvenilir kaynağa dayanmadan dağıtılacak oluşumlar arasında uzlaşma sağlanamaması, aracı bir üçüncü parti yazılım kullanılması gibi çözümler yerine kullanılacak blok zinciri mimarisi ile etkin bir çözüm sunulmaktadır. Blok zinciri teknolojisi hassas veriler üzerinde veri güvenliğini kontrol ederek garanti etmektedir. Bu durum tıbbi alandaki hasta ve farklı aktörler için sağlıklı veri yönetimi kolaylaştırmaktadır. Sağlık hizmetleri ayarlarında, bağlantılı eşler arasında gerçekleştirilen ETK verilerini oluşturma, yükleme veya aktarma işlemi olarak bir işlemi Blok Zinciri mimarisi içerisinde tanımlayabiliriz. Bu mimaride belirli bir zamanda gruplandırılmış işlem kümesi, tüm işlemi kaydeden ve dolayısıyla ağın durumunu temsil eden deftere eklenmektedir. Bu sürecin sağlık hizmetlerinde uygulanmasının temel faydaları şunlardır: veriler doğrulanabilir ve değişmez işlemler için tanımlanır; dağıtılmış hassas tıbbi verilere müdahale edilmesi sürecindeki verilerin şeffaflığı ve bütünlüğü. Bu, temel olarak, mutabakat protokolü, "hash" ve dijital imzalar gibi kripto grafik ilkellerin kullanılmasıyla elde edilmektedir.

## 3. Elektronik Tıp Kayıtlarının Blok Zinciri'nde Tutulması

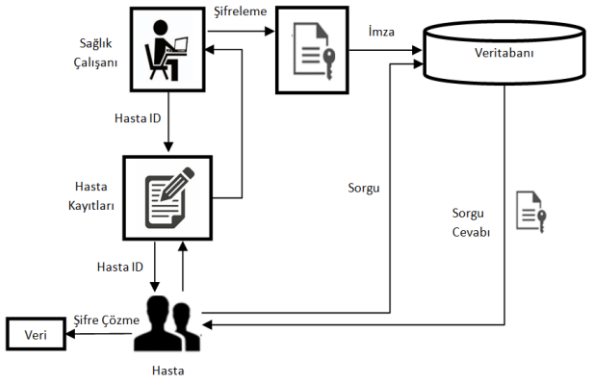
Verilerin bulut ortamına taşınmasıyla bazı politika ve çerçevelere uymak için veri paylaşımı geleneksel erişim kontrolleriyle sağlanmaktadır. Bu erişim yöntemlerinde güvenlik riskleri bulunmaktadır. Bu risklerden korunmak amacıyla veriye erişimin engellenmesi, paylaşım ortamından ayrılması durumunda veriye erişimin durdurulması ve anonim hale getirilen verilere erişimde kullanıcıların tekrar tanımlanması sağlanmaktadır. Gizliliği önlemede ise K-anonimlik, `-Diversity, t-yakınlık teknikleri kullanılmaktadır. Risklerin var olması ve gizliliğin sağlanamaması durumlarında medikal verilerin paylaşılması ve tedavinin gerçekleştirilmesi hasta tarafından engellenebilmektedir. Şekil 3'te gösterilen medikal kayıt ortamlarında tanımlama, kimlik doğrulama ve yetkilendirme ile verilerin paylaşımı gerçekleştirilmektedir. Yetkilendirilen kullanıcılar sahip oldukları rollere kimlik doğrulama ve tanımlama işlemlerinden sonra veriye erişim sağlayabilmektedir. Bu tür sistemler siber güvenlik noktasında savunmasız kalmaktadır (Zhou vd., 2010).




**Şekil 3.** Blokzinciri olmayan Medikal Sistem Tasarımı (Zhou vd., 2010).

Şekil 4'te gösterilen tasarıma sahip blok zinciri mimarisinde veriler şifreli olarak iletilmektedir. Şifrelenen veriler sağlık çalışanı rolüne sahip kullanıcılar tarafından imza ile veritabanına kayıt edilmektedir ya da veritabanındaki veriler güncellenmektedir (Esposito vd., 2018). Aynı zamanda hasta id ile hasta kayıtlarına hasta eklenerek veriye hasta rolündeki kullanıcılar erişim sağlanmaktadır. Bu tarz bir tasarım medikal verilerin blok zincirinde saklanmasında 4 önemli katkıyı beraberinde getirmektedir. Bunlar gizlilik, veri bütünlüğü, güvenlik ve ölçeklene-bilirliktir (Zyskind vd., 2014).

Gizlilik, hastanın mahremiyeti, hastaya verileri üzerinden izinler yoluyla ince taneli erişim kontrolü belirleme olanağı istenerek sağlanmaktadır.




**Şekil 4.** Blok Zinciri Mimarisine Sahip Medikal Sistem Tasarımı (Esposito vd., 2018).

İzinler, zincir kodu mantığı tarafından uygulanmaktadır. Bu nedenle, fikir birliği protokolleri başarısız olmadıkça herhangi bir kullanıcı tarafından ihlal edilememektedir. İkincisi, yalnızca doğrulama düğümlerinin bir kısmı, ağ operasyonlarına zarar vermeye niyetliyse gerçekleşebilmektedir. Merkezi üyelik hizmeti zaten Sybil saldırılarına karşı korumaktadır. Ayrıca, izin verilen ağda düğüm kimlikleri bilinmektedir. Bu nedenle, kötü niyetli davranışlar için bir teşvik bulunmamaktadır. Bir düğümün hala kötü niyetli davranması durumunda, bu düğüm için ağa erişim hemen kısıtlanabilmektedir. Üyelik servisi ayrıca kullanıcıların kimliğini de kontrol etmektedir. Bir uzmanı kaydetmeden önce kimliği Ulusal Uygulayıcı Veri Bankası'nda (UUVB) doğrulanmaktadır. Bir hasta UUVB'ye kayıtlıdır, ancak tüm verileri gizli anahtarı olan takma isimle ilişkilendirilmiştir. Bu nedenle, Üyelik hizmetinin hastanın klinik verilerine erişimi yoktur, ancak kullanıcıların orijinalliğini dijital imza doğrulaması yoluyla garanti etmektedir. Takma isim veri setinin tehlikeye girmesi ya da kaybolması durumunda, ağa erişim bir hastanın UUVB'si kullanılarak kurtarılabilmektedir. Yeni bir anahtar oluşturulmasıyla birlikte vekil sunucu ile yeniden şifreleme kullanılarak sürecin akışı kontrol edilmektedir (Kosba vd., 2016). Medrec isimli çalışmada ise kullanıcıların ve araştırmacıların belirli formları doldurmaları ve eşleştirmeleri sonucu hangi verilerin blok zincirinde tutulacağı belirlenmektedir (Azaria vd, 2016).

Güvenlik, bulut deposunda saklanan klinik veriler, veri gizliliği sağlamak için bir hasta gizli anahtarı olan takma bir isim ile şifrelenmektedir. Sadece hasta şifreleme anahtarı paylaşılmaktadır. Böylece erişim kontrol politikası izinlerle kurabilmektedir. Bulut kayıt defterinden paylaşılan veriler, veriler yüklenmeden önce bir kullanıcının gizli bir

anahtarı ile işaretlenmekte ve imzalanmaktadır. Karma dosyalar durumdaki ilgili bir meta veri öğesinin parçası olarak depolanmaktadır. Ayrıca işlemler dijital olarak imzalanmaktadır. Böylece veri bütünlüğü sağlanmaktadır (Lin vd., 2017).

Verilerin depolanması için bir bulut platformu sağlayarak paylaşılan verilerin kullanılabilirliği garanti edilmektedir. Rol tabanlı uygulama ara yüzleri, zincir kodlarını çağırmak ve sorgulamak için ağda kayıtlı herhangi bir düğümde kullanılabilmektedir. Bir hasta kimlik bilgilerini kaybederse, açık ve kapalı zincirdeki verilere erişim hala kurtarılabilmektedir.

Blok zincirindeki güvenliğin sağlanabilmesi adına paylaşılan veri havuzu yapısı geliştirilmiştir. Bu alanlara erişim kontrolü sağlamak için güvenli şifreleme teknikleri kullanılmıştır. Veri kullanıcılarının ve sahiplerinin, kimlikleri ve şifreleme anahtarları doğrulandıktan sonra paylaşılan depodaki elektronik tıbbi kayıtlara erişim gerçekleşmektedir (Xia vd., 2017).

Klinik veri paylaşımı hem kullanıcı sayısı hem de düğüm sayısı açısından sistemin ölçeklenebilirliğini gerektirir. Bu süreçte aktif olarak kullanılan PBFT protokolü, kullanıcı sayısı açısından ölçeklenebilirliği sağlamaktadır (Xia vd., 2017). Ancak düğüm sayısı arttıkça ölçeklenebilirlik sorunlu hale gelmektedir. Olası ölçeklenebilirlik sorunları, hiyerarşik BFT protokolleri kullanılarak ele alınarak çözümlenmektedir. Bir blokta bir blok veya işlem sayısı oluşturma sıklığı parti boyutu olarak isimlendirilir. Parti boyutu ayarlanabilir durumdadır. Sistem yükü, hastanın klinik kayıtlarının zincir dışı depolanmasıyla en aza indirilmektedir.

## 4. Sonuç ve Tartışma

Bu çalışmada blok zinciri mimarisinin sağlık alanındaki veri sürecinin yönetilebilirliği süreci üzerine araştırma yapılmıştır. Blok zinciri verileri bloklar halinde ve etkileşimli tutmaktadır. Bu blok süreci ve etkileşim ile tüm veriler entegre hale gelmektedir. Verilerde yapılan değişiklikler ve ağın sürekli güncel hale gelmesiyle farklı sağlık kuruluşları olsa da hastaya ait verilere ulaşabilmektedir. Sağlık kuruluşlarının yanı sıra hastalar ve anonim hale gelecek hastaya ait verileri kullanarak araştırma yapacak olan uzman adayları için de entegre bir çözüm blok zinciri mimarisi sunmaktadır. Oluşturulacak mimari izinli ya da izinsiz bir süreç üzerinden tasarlanabilmektedir. İzinsiz blok zinciri mimarisinden hasta uygulaması ve sağlayıcı uygulaması ile süreç yönetilmektedir. API yardımıyla ulaşılan blok zincirinde sürece katılımda bir izin mekanizması bulunmamaktadır. İzinli blok zinciri tasarımında ise ortada yer alan blok zinciri sürecine farklı kullanıcı rolleri ile giriş yapılmaktadır. Roller bir yönetici tarafından belirlenmektedir. Her bir rolün yapacağı işlemler kısıtlanarak erişimde güvenlik bir adım ileriye taşınmaktadır.

Blok zinciri olarak tasarlanmayan bir veri akış sürecinde bulut ortamına çıkılması verilerin güvenliği, bütünlüğü, gizliliği ve ölçeklenebilir olması problemleri yaşanmaktadır. Bu problemlere etkin çözüm üretebilecek kapasiteye sahip blok zinciri tasarımı ile tüm ETK'ler etkin kullanımına olanak sağlanabilecektir. Özellikle hastanın farklı sağlık kuruluşlarındaki teşhis ve tedavi süreçleri birbirine bağlı olarak takip edilebilir ve erişilebilir olarak sürdürülmesine olanak sağlanabilecektir.

Blok zinciri üzerinde geliştirilen medikal uygulamalardan Medrec'te araştırma yapacak kişiler anonimleştirilmiş, büyük ölçekli tıbbi veri kaynağına gizlilik ilkesini bozmadan erişebilmektedirler. Sağlayıcılar, uygun gizliliğin korunması sınırları dahilinde, araştırmacıların kabul etmek istedikleri şeyleri eşleştirmek için teşvik edilmektedir. Hastalar ve sağlayıcılar verilerinin ne kadarının mevcut madencilik işlemine dahil edileceğini sınırlayabilmektedir. Bu durum teşhis ve tedavilerde kullanılan süreçleri gözlemleme fırsatını sunarken, bireylerin mahremiyeti korunmuş olmaktadır. Bir diğer tasarım olan BBDS sisteminde, kullanıcıların kimlikleri ve şifreleme anahtarları doğrulandıktan sonra paylaşılan havuzdan veri istemesine izin vermektedir. Bu durum hem güvenlik hem de veri depolarının etkin kullanımıyla ölçeklenebilirlik problemini çözmektedir (Xia vd., 2017). Bulut ortamında veri bütünlüğünün sağlanması noktasında blok zinciri önemli katkı sağlamaktadır. Madencilik işleminin ardından veriler bir arada ve birbiri ardına eşleşerek bulunmaktadır. Bu zincir bozulduğunda doğrulama yapılmadığından dolayı veri bütünlüğü sağlanmış olmaktadır (Lin vd., 2017).

## Kaynaklar

Azaria, A., Ekblaw, A. ve Vieira, T., 2016. Medrec: Using blockchain for medical data access and permission management, IEEE International Conference on Open and Big Data, 25-30.

Chang, P.Y., Hwang, M.S. ve Yang, C.C., 2017. A blockchain-based traceable certification system, International Conference on Security with Intelligent Computing and Big-data Services, 363-369.

Cruz, J.P., Kaji, Y. ve Yanai, N., 2018. RBAC-SC: Role-based access control using smart contract, IEEE Access, 6, 12240-12251.

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.

Hauxe, R., 2006. Health Information Systems—Past, present, future, International Journal of Medical Informatics, 75, 3-4, 268-281.

He, D., Kumar, N., Wang, H., Wang, L., Choo, K. ve Vinel, A., 2016. A Provably-secure cross-domain handshake scheme with symptoms matching for mobile healthcare social network, IEEE Transactions on Dependable and Secure Computing, 13, 9, 1545-5971.

Karaarslan, E. ve Akbaş, M.F., 2017. blokzinciri tabanli siber güvenlik sistemleri, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3, 2, 16-21.

Kosba,A., Miller,A., Shi E. ve Wen, Z., 2016. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, IEEE Symposium on Security and Privacy, 839-858.

Kuo, A.M.H., 2011. Opportunities and challenges of cloud computing to improve health care services, Journal of Medical Internet Research, 13, 3.

Lee, C.H ve Kim, K.H, 2018. Implementation of IoT system using block chain with authentication and data protection, IEEE International Conference on Information Networking, 936-940.

Lemieux, V.L., 2017. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation, IEEE International Conference on Big Data, 2271-2278.

Liang, X., Shetty, S,. Tosh, D., Foytik P. ve Zhang, L., 2017. Towards a trusted and privacy preserving membership service in distributed ledger using Intel software guard extensions, International Conference on Information and Communications Security, 304-310.

Lin, I.C. ve Liao T.C., 2017. A Survey of blockchain security issues and challenges, International Journal of Network Security, 19, 5, 653-659.

Mandl, K. D., Markwell, D., MacDonald, R., Szolovits, P. ve Kohane, I. S., 2001. Public standards and patients' control: how to keep electronic medical records accessible but private Medical information: access and privacy Doctrines for developing electronic medical records Desirable characteristics of electronic medical records Challenges and limitations for electronic medical records Conclusions Commentary: Open approaches to electronic patient records Commentary: A patient's viewpoint, BMJ, 322,7281, 283-287.

Mengelkamp, E., Notheisen, B., Beer, C. ve Dauer, D., 2018. A blockchain-based smart grid: towards sustainable local energy markets, Computer Science-Research and Development, 33, 1-2, 207-214.

Pavel, C. ve Rajcaniova M., 2018. Virtual relationships: short-and long-run evidence from bitcoin and altcoin markets, Journal of International Financial Markets, Institutions and Money, 52, 173-195.

Poh, G.S., Chin, J., Yau, W. ve Mohamad, M., 2017. Searchable symmetric encryption: designs and challenges, ACM Computing Surveys, 50, 3.

Sara, S., Kouhizadeh, M. ve Sarkis, J., 2018. Blockchain technology: A panacea or pariah for resources conservation and recycling?, Resources, Conservation and Recycling, 130, 80-81.

Steward, M., 2005. Electronic Medical Records, Journal of Legal Medicine, 26, 4, 491–506.

Tang, P.C., Ash, J.S. ve Bates, D.W., 2006. Personal Health Records: Definitions, benefits, and strategies for overcoming barriers to adoption, Journal of the American Medical Informatics Association., 13, 2, 121-126.

The Office of the National Coordinator for Health Information Technology, (2018, 28 Mayıs). Report on health information blocking, https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.

Tschorsch, F. ve Scheuermann, B., 2016. Bitcoin and Beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys and Tutorials, 18, 3, 2084–2123.

Xia, Q., Sifah, E., Smahi, A., Amofa, S. ve Zhang, X., 2017. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments, Information, 8, 2, 44.

Zhang, J., Xue, N. ve Huang, X., 2016. A Secure System for Pervasive Social Network Based Healthcare, IEEE Access, 4, 9239–9250.

Zhou, X., Chen, S., Liu, B., Zhang, R., Wang, Y., Li, P. ve Yan, X., 2010. Development of traditional chinese medicine clinical data warehouse for medical knowledge discovery and decision support, Artificial Intelligence in Medicine, 48, 2-3, 139-152.

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