19. BÖLÜM / CHAPTER 19

SAĞLIKTA BLOK ZİNCİR

BLOCKCHAIN IN HEALTHCARE

Büşra ÖZDENİZCİ KÖSE*

*Dr. Öğr. Üyesi, Gebze Teknik Üniversitesi, İşletme Fakültesi, İşletme Bölümü, Kocaeli, Türkiye

E-mail: busraozdenizci@gtu.edu.tr

DOI: 10.26650/B/ET07.2021.003.19

ÖZ

Günümüzün çarpıcı teknolojik gelişmelerinden biri olan Blockchain (Blok zincir) teknolojisi, birçok endüstriyle beraber sağlık sektörünün dijital dönüşümünde önemli bir rol oynamaktadır. Dijital sağlık paradigmasıyla sağlık sistemlerindeki mevcut geleneksel ve merkezi yaklaşımlar heterojen verilerin yönetimi, veri güvenliği ve birlikte çalışabilirlik konularında yetersiz kalmaktadır. Sağlık ekosisteminde farklı teknoloji platformları ve uygulamalar arasında güvenli bir şekilde veri alışverişi yapabilen, organizasyon sınırları içinde ve ötesinde birlikte çalışabilir bir teknolojik altyapının sağlanması ihtiyacı giderek artmaktadır. Özünde bir Dağıtık Defter Teknolojisi (Distributed Ledger Technology, DLT) olan Blockchain, merkezi bir otorite olmadan, uçtan uca bağlantılı kullanıcılar arasında otomatikleştirilmiş bir uzlaşma sağlayarak değiştirilemez varlık kayıtların oluşturulmasını, güvenli bir şekilde dağıtık mimari ile bu kayıtların paylaşılmasını ve şeffaflık ilkesiyle işlemlerin izlenebilirliğine olanak sağlamaktadır. Birbirine güvenmeyen ve heterojen yapıdaki tarafların bağlantılı dünyasında, her türlü varlık (para, oy, mülk, ürün, fikir, enerji tüketimi, tıbbi öykü ve benzeri) kaydı gerçekleştirilebilir, bu kayıtlar korunabilir ve elektronik ortamda bu varlıkların değişimi sağlanabilir. Son yıllarda sağlık sektöründe, Blockchain teknolojinin katma değerli uygulamaları üzerinde yoğun çalışmalar gerçekleştirilmektedir. Blockchain teknolojisi elektronik ve kişisel sağlık kayıtlarının yönetimi, uzaktan hasta yönetimi, kimlik yönetimi ile entegre akıllı sağlık profillerinin geliştirilmesi, reçetelerin takibi, ilaç ve tıbbi cihaz tedarikinde sahtecilikle mücadele etme, sigorta geri ödeme süreçlerinin denetimi, sağlık verilerinin (tıbbi öykü, tanı, tedavi, DNA kayıtları, yaşam tarzı, fiziksel aktivite gibi) klinik araştırmalarda güvenli kullanımı gibi birçok alanda gelişmektedir. Bu bölüm, sağlık alanında Blockchain teknolojinin potansiyelini keşfetmeyi ve gelişmekte olan uygulama alanlarını kapsamlı bir çerçeve ile sunmayı amaçlamaktadır. Dijitalleşen sağlık alanında güncel ihtiyaçlar, Blockchain teknolojisine genel bakış, bir karar ağacı modeli kapsamında sağlıkta Blockchain teknolojinin önemi, uygulama alanları ve örnekler paylaşılmıştır. Bununla beraber, sürdürülebilir bir Blockchain tabanlı sağlık ekosistemi için çözümlenmesi gereken teknoloji kısıtlarından da bahsedilmektedir.

Anahtar Kelimeler: Blok zincir, dağıtık defter teknolojisi, sağlık, veri güvenliği, birlikte çalışabilirlik, uygulama alanları

ABSTRACT

Blockchain technology, as one of today's fascinating technological developments, plays an essential role in the digital transformation of the health care industry together with many industries. With the digital health paradigm, the existing traditional and centralized approaches in health care systems fall short of heterogeneous data management, data security, and interoperability issues. In the health care ecosystem, there is an urgent need to provide a technological infrastructure that can securely exchange data between different technology platforms and applications, and can work together within and beyond the organizational boundaries. Blockchain, as a Distributed Ledger Technology, enables the creation of immutable asset records by providing an automated consensus among peer-to-peer connected users, by sharing these records with a securely distributed architecture, and by enabling the traceability of transactions with the principle of transparency, without a central authority. In the connected world of parties that do not trust each other and have a heterogeneous structure, all kinds of assets (money, votes, property, product, idea, energy consumption, medical history, etc.) can be recorded and protected; and these assets can be exchanged electronically. In recent years, a large number of studies have been conducted on the value-added applications of blockchain technology in the health care industry. Blockchain technology is evolving in many areas such as the management of electronic and personal health records, remote patient management, development of smart health profiles integrated with identity management, prescription monitoring, prevention of fraud in drug and medical device supply chain, supervision of insurance reimbursement processes, and the safe use of health data (medical history, diagnosis, treatment, DNA records, lifestyle, physical activity, etc.) for clinical trials. This section aims to explore the potentials of blockchain technology in the health care field and present its emerging application domains with a comprehensive framework. Additionally, this study presents the current needs of digitalizing healthcare, an overview of blockchain technology, the significance of blockchain technology in health care within the scope of a decision tree model, application areas, and real-world examples. This study also emphasizes technological constraints that need to be resolved for a sustainable blockchain-based health care ecosystem.

Keywords: Blockchain, distributed ledger technology, health care, data security, interoperability, application domains

1. Giriş

Günümüzde, neredeyse her sektörde daha verimli, etkin ve ekonomik çalışabilmek için dijital dönüşüm (*digital transformation*) kaçınılmazdır. Değişen toplumsal ihtiyaçlar, ekonomik dengeler ve hızla gelişen bilgi ve iletişim teknolojilerinin sunduğu imkanlar kapsamında organizasyonların, süreçlerin, insanların ve mevcut teknoloji altyapılarının kapsamlı, sistematik ve sürdürülebilir dönüşümü konusunda önemli stratejik adımlar atılmaktadır. Mobil teknolojiler, Akıllı Kartlar (*Smart Cards*), Bulut Bilişim (*Cloud Computing*), Büyük Veri (*Big Data*), Kablosuz Algılayıcı Ağlar (*Wireless Sensor Networks- WSN*), Nesnelerin İnterneti (*Internet of Things- IoT*), Yapay Zeka (*Artificial Intelligence- AI*), Artırılmış Gerçeklik (*Augmented Reality- AR*), 3-Boyutlu (*3D*) yazıcılar ve diğer birçok modern teknolojinin hayatımıza girmesiyle daha verimli süreçlerin, yeni iş modellerinin, katma değerli ürünlerin/hizmetlerin elde edilmesi ve gelişmiş insan-bilgisayar etkileşimlerinin oluşması sağlanmıştır.

Sağlık sektöründe de yenilikçi teknolojilerin kullanımı ve dijital dönüşüm yoğun bir şekilde teşvik edilmektedir. Oldukça geniş, dinamik ve heterojen bir yapıya sahip olan sağlık

ekosistemi hastalar, hastaneler, laboratuvarlar, eczaneler, sigorta firmaları, ilaç firmaları, medikal/tıbbi cihaz üreticileri, dağıtıcılar ve benzeri birçok paydaşı barındırmaktadır. Bununla beraber her paydaşın amaçlarına ve gerçekleştirmesi gereken görevlere bağlı olarak çok sayıda ve türde bilgi yönetim sistemleri, veritabanı ve teknoloji platformları kullanılmaktadır. İdeal ve sürdürülebilir bir sağlık ekosisteminde, paydaşlar arasında güven ortamı yaratan; çeşitli teknoloji platformları ve uygulamaları arasında güvenli bir şekilde iletişim kurulabilen ve veri alışverişi yapabilen; organizasyon sınırları içinde ve ötesinde birlikte çalışabilir bir teknolojik altyapının sağlanması gerekir.

Paydaşlar arasında veri paylaşımı ve sistemlerin birlikte çalışabilirliği (*interoperability*) sağlık sektöründeki en önemli konulardan biridir. Bir hastanın birden fazla sağlık kuruluşundan aldığı bakım hizmetlerinin ve sağlık verilerinin entegrasyonu, kalite ve güvenlik sağlamakla beraber acil bakım planlamalarını, hastalığın bakım, tanı ve tedavisine hızlı erişimi kolaylaştırabilir. Sağlık çalışanları, güçlendirilmiş koordinasyon sağlayarak, hasta bakımının kalitesini ve güvenliğini artırabilir; daha iyi karar verme süreçleri gerçekleştirebilir. Diğer yandan, eczane bilgi sistemlerinin birlikte çalışabilirliği veya reçetelerin elektronik ortamda paylaşım, zararlı ilaç etkileşimleri ve olası hataların önüne geçilmesini sağlayabilir. Sigorta şirketleri hızlı ve kaliteli veri entegrasyonları ile hastaların bakım, tanı ve tedavi süreçlerine ve sonuçlarına bağlı olarak maliyetlerde tasarruflar sağlayabilir. Benzer şekilde, sağlık ekosisteminde bulunan diğer birçok paydaş için sağlık bilgi yönetim sistemlerinin birlikte çalışabilirliği ve güvenli veri paylaşımı büyük bir önem arz etmektedir.

Mevcut durumda, sağlık hizmet sağlayıcıları ve sağlık araştırmacıları çok sayıda merkezi veritabanı sistemleri, heterojen veri kaynakları, gecikmeli iletişim ve farklı iş akışlarıyla mücadele etmektedir (Zhang vd., 2018; Agbo vd., 2019; McGhin vd., 2019). Paydaşlar yüksek gizlilik ve güvenlik ile merkezi veritabanlarında korudukları sağlık verilerini, uçtan uca bağlantılar oluşturarak güvenli bir şekilde değiştirme konusunda sıkıntılar yaşamaktadır. Güvenilir sistemler arasında iletişim için kullanılan HL7 (*Health Level Seven-Sağlık Seviye 7*), FHIR (*Fast Healthcare Interoperability Resources*) gibi veri standartları belli seviyelerde birlikte çalışabilirlik sağlamasına rağmen, bu birlikte çalışabilirlik uygulanan standartlarla sınırlı kalabilmektedir. Farklı teknoloji platformları, ağ yapıları, erişim kontrol ve sistem güvenlik mekanizmaları, uyumsuz yazılımlar gibi faktörler sağlık verilerinin eşleşmesini ve sistemlerin birlikte çalışabilirliğini zorlaştırabilmektedir. Bu kapsamda, sağlık sektöründe paydaşlar arası iletişim koordinasyonunu daha verimli hale getirecek, hasta bakım kalitesini artıracak, bireylerin ve toplulukların refahını sağlayacak güvenli, birlikte çalışabilir ve sürdürülebilir teknolojik altyapılara ihtiyaç vardır.

Günümüzün çarpıcı teknolojik gelişmelerinden biri olan blok zincir (*blockchain*) teknolojisi de, birçok endüstriyle beraber sağlık sektörünün dijital dönüşümünde önemli bir potansiyele sahiptir. Blok zincir teknolojisi, 2009 yılında Satoshi Nakamoto takma adlı bir kişi veya kurum tarafından ilk ve en büyük merkezi olmayan kriptopara (*cryptocurrency*) birimi Bitcoin ile gündeme gelmiştir (Nakamoto, 2018). Bitcoin, internet üzerinden merkezi olmayan bir sistemde, kamuya açık, paylaşılan bir hesap defteri - yani blok zincir altyapısı - kullanılarak işlem gören bir dijital para olarak tanımlanmaktadır (User & User, 2019). Bitcoin teknolojinin piyasaya sürülmesinden sonra çeşitli alternatif kriptopara birimleri ortaya çıkmıştır ve çeşitli uygulamalar geliştirilmiştir. Kriptopara teknolojilerinin temelini oluşturan blok zincir, kısa zaman içerisinde çeşitli amaçlarla kullanılabilecek bir teknoloji haline gelmiştir.

Blok zincir teknolojisinin popülerlik kazanmasındaki en önemli özelliklerinden biri, kullanıcıların birbirlerine güven duyma ihtiyacını gerektirmemesi ve merkezi bir otoriteye bağlı olmamasıdır. Özünde bir Dağıtık Defter Teknolojisi (*Distributed Ledger Technology, DLT*) olan blok zincir, merkezi bir otorite kullanmak yerine, ademi merkeziyetçilik ortamında, uçtan uca (*Peer to Peer-P2P*) bağlantılı kullanıcılar arasında otomatikleştirilmiş bir anlaşma ve fikir birliği (*consensus*) sağlamaktadır. Bu dağıtık mimari - yani dağıtık defter - üzerinde değişmez (*immutable*) veri kayıtlarının oluşturulmasına, verilerin güvenli (*secure*) bir şekilde saklanmasına ve şeffaflık (*transparency*) sağlayarak verilerin izlenebilirliğine (*traceability*) olanak sağlamaktadır (Zheng vd., 2018; Nguyen vd., 2019; Fernández-Caramés & Fraga-Lamas, 2018). Sahip olduğu bu özelliklerle blok zincir, yeni bir bağlantılı bilgi işlem paradigmasını karımıza çıkarmaktadır: Birbirine güvenmeyen ve birbirinden farklı (heterojen yapıda) tarafların bağlantılı dünyasında, merkezi bir otorite olmadan her türlü varlık (para, oy, mülk, ürün, fikir, enerji tüketimi, tıbbi öykü ve benzeri) kaydı gerçekleştirilebilir, bu kayıtlar korunabilir ve elektronik ortamda bu varlıkların değişimi sağlanabilir.

Dünya çapında finans, sigorta, üretim, tedarik zinciri, enerji gibi birçok endüstri alanında avantajları öngörülen blok zincir teknolojisinin, son yıllarda sağlık sektöründeki katma değerli uygulamaları üzerinde yoğun çalışmalar gerçekleştirilmektedir. Sağlık ekosisteminde mevcut birlikte çalışabilirlik sorunlarını çözerek güvenli ve değiştirilemez bir sağlık kaydı deposu oluşturma; hastalar, sağlık hizmeti sağlayıcıları, sigorta firmaları ve diğer birbirine güvenmeyen paydaşlar arasında varlıkların güvenli bir şekilde paylaşılması, varlık envanterinin tutulması ve izlenmesi gibi konularda çeşitli uygulamalar geliştirilmektedir.

Bu bölüm, araştırmacılara ve uygulayıcılara sağlık alanında blok zincir teknolojisinin potansiyelini ve uygulama alanlarını kapsamlı bir çerçeve sunmayı amaçlamaktadır. Bu kapsamda, blok zincir teknolojisinin sağlık sektöründeki temel uygulama alanları ve uygulama

alanlarına katkıları, gerçek uygulama örnekleriyle beraber paylaşılmaktadır. Aynı zamanda, blok zincir teknolojisinin sağlık alanındaki mevcut teknoloji yol haritasının anlaşılmasıyla, gelecekte sürdürülebilir bir blok zincir tabanlı sağlık ekosistemi için hangi teknolojik kısıtların çözümlenmesi gerektiği konusunda okuyucular bilgilendirilecektir.

Bu kapsamda bu bölümün geri kalanı şu şekilde düzenlenmiştir: Bölüm 2’de sağlık sektöründe - blok zincir teknolojisinin potansiyelini ve kullanımını adresleyen - güncel gereksinimler ve konular paylaşılmaktadır. Ardından, Bölüm 3’te blok zincir teknolojisinin teknik bileşenleri ve genel çalışma yapısı tanımlanmaktadır. Bölüm 4’te, sağlık alanında blok zincir teknolojisinin kullanım uygunluğu konusu bir karar modeli ile değerlendirilmektedir. Bölüm 5’te, sağlık alanında blok zincir teknolojisinin güncel uygulama alanları, sağladığı faydalar ve örnek uygulamalar dört ana kategoride incelenmektedir. Bölüm 6’da, blok zincir teknolojisinde geliştirilmesi veya çözümlenmesi gereken mevcut kısıtlardan bahsedilmektedir ve Bölüm 7 genel bir bakış ile kitabın bu bölümünü sonlandırmaktadır.

2. Sağlık Alanındaki Gelişmeler ve Gereksinimler

Bu bölüm, sağlık ekosisteminde blok zincir teknolojisinin kullanımını adresleyen mevcut gelişmeleri ve temel gereksinimleri iki perspektifte incelemektedir: (1) sağlık verilerinin yönetimi ve güvenliği; (2) sağlık verilerinin paylaşımı ve birlikte çalışabilirlik.

2.1. Sağlık Verilerinin Yönetimi ve Güvenliği

Sağlık ekosistemi hastalar, sağlık hizmeti sağlayıcıları, sigorta firmaları, ilaç firmaları, eczaneler, araştırmacılar ve benzeri birçok paydaşı içermektedir. Her bir paydaş tarafından elektronik ortamlara aktarılan, üretilen, depolanan ve paylaşılan çok sayıda elektronik sağlık (*electronic health - e-Health*) verisi bulunmaktadır. Bu büyük verinin kullanımı konusunda paydaşların belli birtakım sorumlulukları vardır. Bir sağlık hizmeti sağlayıcısı, bir bireye tanı ve tedavi işlemleri gerçekleştirirken çeşitli kişisel verilere erişir; bireye ait yeni sağlık verileri tanımlar; ve hatta bu verilerin kalıcı olarak çeşitli merkezi veritabanı sistemlerinde depolar. Bir bireyin, birden çok sağlık hizmeti sağlayıcısı ile etkileşim gösterdiğini düşündüğümüzde, farklı platformlarda oluşan Elektronik Sağlık Kayıtlarının (*Electronic Health Records-EHR*) koruması oldukça önemlidir. T.C. Sağlık Bakanlığı (2014) tarafından Elektronik Sağlık Kaydı, “*kişilerin geçmişteki, şimdiki ve gelecekteki fiziksel ve ruhsal sağlığı veya hastalıkları ile ilgili elektronik sistemler kullanılarak kayıt altına alınan, saklanan, iletilen, erişilen, ilişkilendirilen ve işlenen her türlü bilgi*” olarak tanımlanmaktadır. Bu kayıtlar, kişiye ait gizli ve hassas verilerdir.

Bu kapsamda, sağlık hizmeti sağlayıcılarındaki Elektronik Sağlık Kayıtlarının korunması ve gizliliğinin sağlanmasıyla ilişkili pek çok gereksinimler ve yasal zorunluluklar bulunmaktadır. *HIPAA (Health Insurance Portability and Accountability Act, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası)*, *GDPR (General Data Protection Regulation, Genel Veri Koruma Tüzüğü)*, Kişisel Sağlık Verileri Hakkında Yönetmelik gibi gizlilik düzenlemelerini ihlal etmeden tıbbi verilerin veya hasta dosyalarının elektronik ortamda korunması (*data-at-rest*) ve paylaşımının (*data-in-motion*) gerçekleştirilmesi çalışılmaktadır.

Geleneksel sağlık sistemlerinde, bir sağlık hizmet sağlayıcısı, bir hastanın verilerini aldıktan sonra, bu verilere kalıcı olarak sahip olur. Bununla birlikte, yine aynı hasta birden çok sağlık hizmet sağlayıcısı değiştirirse, birçok farklı sağlayıcı hassas sağlık verilerine sahip olacaktır. Bu durum, veri gizliliğini tehdit edebilir ve hatta veri hırsızlığı olasılığını artırabilir. Diğer taraftan, aynı hasta, farklı bir sağlık hizmet sağlayıcısının kendisine ait sağlık verilerinin hepsine ve bir kısmına erişmesini isteyebilir; yani kendisine ait verileri yönetmek isteyebilir. Fakat, geleneksel sistemlerde, verileri hızlıca paylaşmak ve daha sonra sağlayıcılar arasında bu verilere erişim kontrolünü sağlamak kolay bir süreç değildir. Diğer bir deyişle, günümüz sağlık sistemleri - hasta merkezli (*patient-centered*) bir yaklaşım yerine - daha çok hizmet sağlayıcı merkezli bir yapıdadır (Zhang vd., 2018; McGhin vd., 2019; Höbl vd., 2018). Bir hastanın hassas verilerinin kontrolsüz ve izinsiz bir şekilde yayılmasının çok ciddi sonuçları olabilir. Sağlık kayıtlarının “hasta kontrolünde” korunması ve güvence altına alınması, gizlilik (*privacy*) açısından bir gerekliliktir.

Günümüzde karşılaşılan diğer bir konu da, kişisel bulut tabanlı depolama ortamlarının artışı; akıllı cihazlar, akıllı telefonlar, algılayıcılar, giyilebilir teknolojiler ve diğer Internet tabanlı cihazların yaygın kullanımıdır. Böylece, hastalar tarafından kullanılan (hastane ve randevu yönetimi, sağlık yaşam, fitness, fiziksel aktivite ve benzeri içerikli) mobil uygulamalar ile daha çok Kişisel Sağlık Kayıtları (*Personal Health Records - PHR*) oluşturma; başka sistemlerde bulunan sağlık verilerine daha hızlı erişme; çeşitli alanlarda bu verileri depolama gibi kavramlar hayatımıza girmiştir. Mobil sağlık (*mobile health, m-health*) ile veri çeşitliliğinin ve hareketliliğinin (*mobility*) artması, farklı ortamlarda verilerin depolanması gibi durumlar söz konusu kişisel verilerinin paylaşımını ve gizliliğini daha da riskli hale getirmektedir (Zhang vd., 2018; McGhin vd., 2019). Bu veri difüzyonu ve heterojen yapı nedeniyle, farkında olmadan, hassas verilerimiz kötü niyetli saldırılara karşı savunmasız bir hale getirilebilir.

Hassas verilerin kullanıma yönelik yasaların ve düzenlemelerin ötesinde; hastaların kendilerine ait tüm sağlık kayıtlarını daha bütüncül ve entegre bir ortamda kontrol edebilmesi, kendilerine ait verilerle neler yapılabileceğini yönetebilmesi ya da verilerine hangi paydaş-

ların eriştiği hakkında bilgi sahibi olması bir ihtiyaçtır. Bu ihtiyacın karşılanması için hasta merkezli bakım yaklaşımını destekleyen güvenli ve izlenebilir sağlık veri yönetim sistemi ve teknolojik altyapı gerekmektedir (Zhang vd., 2018; Höbl vd., 2018).

Böyle bir sistem kapsamında kullanıcılarının kimlik doğrulaması (*authentication*), yapılan işlemlerin inkar edilememesi (*non-repudiation*), erişim kontrolü (*access control*), veri bütünlüğü (*data integrity*) gibi başlıca güvenlik gereksinimlerinin karşılanması gerekir. Kimlik yönetimi ve kimlik doğrulaması her bilgi sistemi için kaçınılmaz bir güvenlik gereksinimidir. Sağlık bilgi sistemi kullanıcılarının kimlik yönetiminin ve bununla beraber ilgili sistem üzerinde kullanıcı tarafından yapılan her işlemin güvenli bir kaydının depolanması gerekmektedir. Kullanıcının gerçekleştirdiği her işlemin, ilgili kullanıcı tarafından reddedilmez ve inkar edilemez bir işlem olarak kaydedilmesi de diğer önemli bir gereksinimdir. Kimlik yönetiminin yanı sıra, farklı veri kaynaklarından gelen sağlık verilerinin depolama ortamındaki güvenliğini artırmak için, rol tabanlı ayrıcalıkların ve erişim kontrol mekanizmalarının oluşturulması gerekir. Hangi verilere kimlerin erişim sağlayabileceğinin tanımlanması, erişim yetkisine sahip tarafların belirlenmesi ve özellikle hastalara ait hassas verilerin hasta kontrolünde etkin bir şekilde yönetilmesi gerekir. Diğer önemli bir güvenlik gereksinimi de veri bütünlüğüdür. Sağlık verilerinin güçlü kriptografi ve şifreleme yöntemleri ile - veri paylaşımında birlikte çalışabilirliği de sağlayacak şekilde - saklanması önemlidir.

2.2. Sağlık Verilerinin Paylaşımı ve Birlikte Çalışabilirlik

Sağlık bilgi sistemlerinin örgütsel sınırlar içinde çalışmasının yanı sıra, örgütsel sınırların ötesinde uyumlu bir şekilde birlikte çalışabilmesi, sunulan sağlık hizmetlerinin verimliliği demektir. Sağlık ekosisteminin, sağlık uzmanlarının hasta vakaları hakkında bilgi paylaşarak etkili ve işbirlikçi tedavi planları belirlemek, bakım kararları almak, hasta ihtiyaçlarını anlamak, tanı doğruluğunu artırmak, ilaç etkileşimlerini tanımlamak, yanlış ilaç kullanımlarını önlemek, ilaç kullanım takibini sağlamak, tıbbi cihaz uygunluğunu kontrol etmek, sağlık sigortası doğruluğunu sağlamak ve diğer birçok amaçla veri paylaşımı (*data sharing*) gerçekleşmektedir. Güvenli ve ölçeklenebilir veri paylaşımı, birlikte çalışabilirlik gerektirir.

HIMSS (Healthcare Information and Management Systems Society - Sağlık Bilgi ve Yönetim Sistemleri Topluluğu) tarafından birlikte çalışabilirlik kavramı şu şekilde tanımlanmaktadır: dünya çapında bireylerin ve toplumların sağlığını optimize etmek ve zamanında kesintisiz veri taşınabilirliğini sağlamak amacıyla, - kurumsal, bölgesel ve ulusal sınırlar içinde veya ötesinde - farklı bilgi sistemlerinin veya cihazların verilere koordineli bir şekilde erişebilmesi, değiştirebilmesi, entegre edebilmesi ve işbirliği içinde kullanabilmesidir (HIM-

SS, 2020). Diğer bir ifadeyle, birlikte çalışabilirlik veriyi alan sistemin, gönderen sistemden aldığı veriyi başka bir işleme gerek kalmadan işleyebilme ve kullanabilme yeteneğidir (Sağlık Bakanlığı, 2015).

Sağlık hizmetlerinde birlikte çalışabilirlik kavramı dört temel seviyede ele alınmaktadır (HIMSS, 2020): temel birlikte çalışabilirlik (*foundational interoperability*), yapısal birlikte çalışabilirlik (*structural interoperability*), anlamsal birlikte çalışabilirlik (*semantic interoperability*) ve örgütsel birlikte çalışabilirlik (*organizational interoperability*).

(1) Temel birlikte çalışabilirlik (Seviye 1), birlikte çalışabilirliğin en temel katmanıdır. Bir bilgi sisteminin başka bir bilgi sistemine güvenli bir şekilde veri gönderme yeteneğidir. En önemli nokta, alıcı bilgi sisteminin, değiştirilen verileri yorumlayabilmesi gerekmez; sadece veri mesajının alındığını onaylayabilmelidir.

(2) Yapısal birlikte çalışabilirlik (Seviye 2), değiştirilecek sağlık verilerinin yapısını ve sözdizimini (*syntax*) tanımlar. Değişimi gerçekleştirilen verinin anlamının korunmasını ve önceden tanımlanmış formatların kullanılmasıyla verilerin yorumlanabilir olmasını sağlar.

(3) Anlamsal birlikte çalışabilirlik (Seviye 3), sadece sözdizimi veya yapısı ile değil, verilerin anlambilimi (*semantic*) ile yorumlanabilir olmasını sağlar. Ortak modeller ve özel kodlamalar ile verilere ait standart tanımlar oluşturur; kullanıcılara ortak bir anlayış ve anlam sağlar. Temel ve yapısal birlikte çalışabilirlik, anlamsal birlikte çalışabilirlik için önkoşuldur. Bu özel kodlama standartları ve modeller olmadan, bilgi sistemleri tarafından bu sağlık verileri kolayca yorumlanamaz.

(4) Örgütsel birlikte çalışabilirlik (Seviye 4) ise kuruluşlar, kurumlar ve bireyler arasında güvenli, kesintisiz ve zamanında iletişim gerçekleştirmek ve veri kullanımını kolaylaştırmak için yönetim, politika, sosyal, yasal ve organizasyonel hususları içerir. Bu bileşenler son kullanıcı süreçleri ve iş akışlarını tanımlar.

Bilindiği üzere, sağlık sistemleri arasında birlikte çalışabilirlik gereksinimi, bazı ortak standartların kullanılması ile sağlanmaktadır. Söz konusu gereksinimleri karşılamak amacıyla ISO (*International Standards Organisation*), CEN (*Comité Européen de Normalisation*), HL7, OpenEHR, IHE (*Integrating the Healthcare Enterprise*) gibi önemli organizasyonlar tarafından mesajlaşma, terminoloji, doküman, kavramsal, uygulama, mimari gibi kategorilerde bir dizi birlikte çalışabilirlik standardı geliştirilmiştir. Ülkemizde de birlikte çalışabilir sağlık bilgi sistemleri oluşturmak amacıyla USVS (Ulusal Sağlık Veri Sözlüğü), SKRS (Sağlık Kodlama Referans Sunucusu), LOINC (*Logical Observation Identifiers Names and Codes*,

Mantıksal Gözlem Tanımlayıcıları İsimleri ve Kodları), ICD-O (*International Classification of Diseases-Oncology*; Uluslararası Hastalık Sınıflandırması-Onkoloji) gibi çeşitli standartlar kullanılmaktadır (Sağlık Bakanlığı, 2015).

Geleneksel merkezi sağlık sistemlerinin kullanımına devam edilmesi ve diğer taraftan sağlık veri kaynaklarının ve çeşitliliğinin artışı, söz konusu büyük ölçekli veri kümelerinin paylaşımı sürecinde ölçeklenebilirlik ve birlikte çalışabilirlik sorunlarını gündeme getirmektedir (Şekil 1). Hatta heterojen veri kaynaklarının artışı ve farklı veritabanları, veri paylaşım sürecinde paydaşlar arasında güven eksiliğine neden olmaktadır. (Zhang vd., 2017; Zhang vd., 2018; McGhin vd., 2019). Hasta merkezli bir sağlık hizmeti modelini ve hasta kontrolünde bir sağlık veri yönetimini desteklemek için, birlikte çalışabilirlik ve güven ilişkisi oldukça önemlidir.

Söz konusu heterojen sistemler arasında veri paylaşımının sorunsuz ve güvenli bir şekilde gerçekleşebilmesi için kapsamlı bir veri eşlemesi gerekmektedir. Mevcut birlikte çalışabilirlik standartları, belli sağlık sistemleri arasında veri paylaşımına imkan sağlamaktadır. Farklı teknoloji platformları, ağ yapıları, güvenli uçtan uca bağlantıların olmaması, farklı şifreleme ve güvenlik mekanizmaları, uyumsuz yazılımlar gibi faktörler sağlık verilerinin eşleşmesini ve sistemlerin birlikte çalışabilirliğini zorlaştırabilmektedir.

Şekil 1. Heterojen Veri Kaynakları (Zhang vd., 2017)

Güven ortamı, sağlık ekosisteminde diğer önemli bir gereksinimdir; güvensiz bir ortamda veri paylaşımı mümkün değildir. Sağlık hizmet sağlayıcıları arasında veya sağlık hizmet sağlayıcısı ile sigorta firması arasında, bir hasta ile ilgili gizli veri iletişimi gerçekleşmeden

önce tarafların iletişim kurulacak sisteme güvenmeleri gerekir. Sonuçta, veri paylaşımı sürecinde yaşanabilecek bir sorunda, sağlık verileri tehlikeye girdiğinde sağlık hizmet sağlayıcıları ve diğer ilgili paydaşlar ciddi mali ve yasal sonuçlarla karşılaşabilirler. İdeal bir sistemde, tarafların kimliklerinin doğrulanması, gerçekleşen işlemlerin inkar edilememesi, şeffaflığı, izlenebilirliği ve denetlenebilirliği güven ilişkisini güçlendirir.

3. Blok Zincir Teknolojisine Genel Bakış

Blok zincir teknolojisinin, sağlık ekosisteminde mevcut ihtiyaçları karşılama ve birbirine güvenmeyen paydaşlar arasında hassas sağlık verilerinin güvenli bir şekilde korunması ve paylaşılması konularında, önemli bir rol oynayacağı öngörülmektedir. Bunu anlamak için blok zincir teknolojisinin öncelikle teknik özelliklerini, temel çalışma yapısını ve avantajlarını anlamaya çalışmamız uygun olacaktır.

2009 yılında kriptopara birimlerinin altyapısını oluşturan halka açık bir Dağıtık Defter Teknolojisi olarak karşımıza çıkan blok zincir (Nakamoto, 2008), kısa zamanda içerisinde birçok sektörde ekonomik, siyasi, yasal ve toplumsal faaliyetlerin yeniden yapılandırılmasında etkili bir teknoloji olduğunu açıkça ortaya koymaya başlamıştır. Blok zincir teknolojisinin gelişimi, üç temel evrede tanımlanmaktadır (Burgess & Colangelo, 2015; Swan, 2015; User & User, 2019): *Blockchain 1.0*, *Blockchain 2.0* ve *Blockchain 3.0*.

Blockchain 1.0, kriptopara birimlerinin altyapısını sağlayacak şekilde blok zincir teknolojisinin, dijital para transferi ve ödeme sistemleri uygulamalarında kullanımınıdır. Bitcoin, Litecoin, Dogecoin, Ripple, NXT, Peercoin kriptopara birimleri örnek olarak verilebilir. Temel amaç, para ve ödemelerin merkezsizleştirilmesi içindir. *Blockchain 2.0* ise, piyasaların daha genel bir şekilde merkezsizleştirilmesi amacıyla - kriptoparanın ötesinde - diğer birçok varlık türü için Blockchain altyapısının kullanımına odaklanmaktadır. *Blockchain 2.0* hisse senetleri, tahviller, vadeli işlemler, krediler, ipotekler, tapular ve benzeri alanlarda, Akıllı Sözleşmeleri (*Smart Contracts*) sağlayacak şekilde blok zincir teknolojisinin finans ve piyasa uygulamalarında kullanımınıdır. *Blockchain 3.0* ise devlet, sağlık, bilim, eğitim, kültür, sanat alanlarında - para, finans ve piyasa uygulamalarının ötesinde - blok zinciri teknolojisinin kullanımınıdır.

Blok zincir, tek merkeze dayalı güven sistemlerindeki merkeziyetçilik yapısını dağıtarak, uçtan uca bağlantılı kullanıcılar arasında dağıtık ve paylaşılan bir kayıt defteri teknolojisidir (Tübitak Bilgem, 2020). Günümüzün önemli bir problemi olan tek bir otoriteye veya merkeze dayalı sistemlerin aksine, Şekil 2’de gösterildiği üzere blok zincir, merkezi olmayan ve dağıtık bir ağ mimarisi ile çalışır. Bu dağıtık ortamda, otomatikleştirilmiş bir fikirbirliği/uzlaşma, güven ve şeffaflık sağlar. Birbirine güvenmeyen ve birbirinden farklı yapıdaki taraflara, mer-

kezi bir otorite olmadan her türlü varlık kaydını gerçekleştirmesine, değiştirilemez verilerin depolanmasına ve güvenli varlık değişimine imkan sağlamaktadır.

Şekil 2. Merkezi Kayıt Defteri ve Dağıtık Kayıt Defteri

Bir blok zincir sisteminin oluşmasını ve işleyişini sağlayan belli birtakım bileşenler vardır: blok zincir oluşturan bloklar (*blocks*), bu blokları oluşturan kayıtlar ve işlemler (*transactions*), bu blokların sakladığı düğümler (*nodes*), uzlaşma protokolleri (*consensus protocols*), Akıllı Sözleşmeler. Şimdi bu bileşenleri inceleyelim.

3.1. Dağıtık Kayıt Defteri: Kayıtlar, Bloklar ve Düğümler

Blok zincir sistemi üzerinde kullanıcılar tarafından gerçekleşen her türlü işlemin içerik bilgisi, bir kayıt olarak saklanır. Kriptopara birimlerinde (örneğin Bitcoin sisteminde) oluşan kayıtlar, gerçekleşen para transferi işlemine ait bilgilerdir. Blok zincir sisteminde bulunan kullanıcılar (diğer bir deyişle katılımcılar) arasında yapılmış olan işlemler, bu kayıtlar ile saklanır. Yani blok zincir sisteminde yapılacak işlemlere bağlı olarak müşteri kaydı, reçete, sağlık test sonucu, tanı bilgisi, tedavi işlemi, sigorta ödeme bilgisi, sağlık raporu, doktor tavsiyesi ve benzeri kayıtlar da saklanabilir.

Blok zincir sistemini oluşturan en önemli yapılar bloklardır. Katılımcılar tarafından oluşturulan kayıtlar, blok zincir sisteminde bir daha değiştirilmemek üzere blok haline getirilmektedir. Sistem üzerinde yapılan işlemlerin karşılığı olan kayıtlar, belirli aralıklarla işlenerek blokların içine yazılır ve bir blok dizisi oluşturulur (Beck, 2018; Singh & Singh, 2016). Her blok oluşturulurken, ilerleyen bölümlerde paylaşılacak olan bazı önemli kriptografi teknikleri kullanılır.

Şekil 3'te gösterildiği üzere, her blok kendisinden bir önceki bloğa, bir referans değer (önceki bloğun özeti) ve zaman damgası (*timestamp*) ile zincirlenir. Her blokta genel olarak iki alan bulunmaktadır: blok başlığı (*block header*) ve blok gövdesi (*block body*).

Şekil 3. Blok Yapısı

Blok başlığı, Tablo 1’de açıklandığı üzere, ilgili bloğu tanımlayan bilgileri içerir. Blok gövdesi ise, ilgili bloğun içerdiği kayıtlardan oluşmaktadır. Bir blok zincirindeki, ilk oluşturulan bloğa Akıllı Blok (*Genesis Block*) denir. Akıllı Blok dışındaki her blok, bir önceki bloğun özet bilgisini içermektedir ve kronolojik bir sırada, doğrusal olarak birbirine bağlanmaktadır. Bir bloğun içerebileceği maksimum kayıt sayısı, blok zincir sisteminin tasarımına, blok büyüklüğüne ve her bir işlemin büyüklüğüne bağlıdır (Zheng vd., 2017; Zheng vd., 2018; Tanrıverdi vd., 2019).

Tablo 1. Blok Başlığı		
Alan	Uzunluğu	Açıklama
Versiyon (<i>Version</i>)	4 bayt	Blok doğrulama kuralları bilgisi
Önceki Bloğun Özeti (<i>Previous Hash</i>)	32 bayt	Bir önceki bloğun başlığının özetleme fonksiyonu çıktısı
Merkle Kökü (<i>Merkle Root</i>)	32 bayt	Blok kayıtlarının Merkle-Ağacı kökünün özet değeri
Zaman Damgası (<i>Timestamp</i>)	4 bayt	Bloğun yaklaşık oluşturulma zamanı
Zorluk Derecesi (<i>Difficulty Target</i>)	4 bayt	Blok için uzlaşma algoritmasının zorluk hedefi
Nonce	4 bayt	Genellikle 0 ile başlayan her bir hesaplama için artan bir sayı

Sistemin diğer önemli bir bileşeni de düğümlerdir. Uçtan uca bağlantılı düğümler, dağıtık mimariyi oluşturur (Şekil 2). *Peer to Peer* (P2P) ağında, her bir bilgisayar sistemi yani kullanıcı bir eştir ve tüm kullanıcılar birbirine eşit kabul edilir. Blok zincir ağında bu eşler, yaygın olarak düğümler (*nodes*) olarak adlandırılan bir makinedir. Her eş, herhangi bir mer-

kezi sunucu gibi bir koordinasyona gerek olmadan, disk depolama, işlem gücü veya ağ bant genişliği gibi bilgisayar kaynaklarının bir kısmını doğrudan diğer katılımcılara sunarak veri dağıtımını ve paylaşımını sağlar (Atabaş, 2018).

Blok zincir sisteminde blok dizisi şeklinde oluşturulan kayıt defterinin - yani veritabanının - kopyası, tüm katılımcılara açık bir şekilde paylaşılmaktadır. Kayıt defteri, blok zincir sisteminin değiştirilemez bir geçmişiştir. Her düğüm, kayıt defterinin kopyasını saklar; aynı zamanda ağ üzerinde gerçekleşen işlemlerin doğrulanması ve onaylanması işlemine katkıda bulunur. Düğümler, blok zincir sisteminin bütünlüğünü korumaktadır. Bir blok zincir ağında ne kadar çok düğüm bulunursa, o kadar güvenli bir hale gelir; çünkü ilgili kayıt defteri üzerinde o kadar çok katılımcının fikir birliği olduğunu gösterir.

Geleneksel merkezi veritabanı mimarisinde üçüncü güvenilir bir taraf ile veritabanı sisteminin kontrol edilmesi sağlanırken (Şekil 2); blok zincir sisteminde düğümler arasında doğrulanan blokların sistematik bir biçimde birbirine eklenmesiyle veritabanı işler ve çalışır. Düğümler arasında paylaşılan kayıt defteri (*shared ledger*), değiştirilemez kayıtlar ve şeffaflık sağlamaktadır. Diğer bir ifadeyle, sistem siber saldırılar, güç kesintileri, sistem çökmeleri ve benzeri durumlara karşı oldukça dayanıklı ve sağlam bir mimariye sahiptir. Sistemdeki herkesin doğrulama yapabildiği bu mimaride, katılımcıların birbirine güvenmesine gerek duyulmamaktadır; çünkü doğru bilginin tutulduğu ispatlanabilir. Bu kapsamda, blok zincir sistemi oldukça geniş bir ekosistem olan sağlıkta - hastalar, hastaneler, laboratuvarlar, sigorta firmaları, ilaç firmaları, dağıtıcılar, eczaneler ve benzeri aktörlerin - işbirliği yapmak istediği uygulamalar için oldukça güvenilir - noter gücünde - bir kayıt ortamı sağlamaktadır.

3.2. Güvenlik Araçları

Blok zincir teknolojisinin dağıtık kayıt defteri mimarisinin temeli, kriptografi üzerine inşa edilmiştir. Merkezi bir otorite olmadan bir sistemin güvenliğini sağlamak amacıyla, kriptografi oldukça önemlidir. Kriptografinin kullanım amacı hem kayıtları oluşturan kullanıcıların kimliğini güvence altına almak, hem de dağıtık veritabanında saklanan işlem kayıtlarının güvenliğini sağlamaktır. Temel olarak kullanılan güvenlik araçları kriptografik özetleme algoritmaları (*cryptographic hash functions*) ve dijital imza (*digital signature*) teknikleridir. Bununla beraber, blok zincir temelli işlemlerin güvenliğini ve gizliliğini artırmak için, isteğe bağlı olarak *Ring Signature*, *Zero-Knowledge Proof* ve benzeri araçlar da kullanılmaktadır.

Şekil 2’de bahsettiğimiz üzere, her blok kendisinden bir önceki bloğa, bir referans değer ve zaman damgası ile bağlanır. Yani, kendisinden önceki bloğun bir özetleme algoritması (genellikle double-SHA-256 algoritması) ile elde edilen özet değeri (*hash*) ile zincirlenir. Özetleme

fonksiyonu (*hash function*), farklı uzunluklardaki verilerin belirli bir uzunluğa dönüştürülmesini sağlayan ve aynı girdi ile her zaman aynı çıktıyı veren tek yönlü fonksiyondur. İdeal bir özetleme algoritmasında, herhangi bir veri girişi için kolayca bir özet değer üretilebilirken, üretilen özet değer kullanarak orijinal verinin bulunması imkansızdır. Bununla beraber orijinal veride yapılabilecek herhangi bir değişiklik sonucunda özet bilgisinde farklılaşma olacağından, özetleme fonksiyonlarının blok zincir sistemlerinde veri bütünlüğünün kontrol edilmesinde ve sağlanmasında çok önemli bir yeri bulunmaktadır (Wang vd., 2019; Gupta, 2017).

Sistem üzerinde kayıtların imzalanması ve doğrulanması için, asimetrik kriptografi yani asimetrik şifreleme mekanizmasına dayalı dijital imza tekniği kullanılır. Elektronik ortamda iletilen bir belgenin hem içeriğini hem de gönderen tarafın kimliği doğrulamak amacıyla ilgili belgeye eklenen dijital bir koddur (Diffie & Hellman, 1976). Blok zincir sisteminde, her kullanıcı bir çift özel ve açık anahtara sahiptir. Katılımcı tarafından yapılan bir işlem katılımcıya ait - gizli tutulan - özel anahtar (*private key*) ile dijital olarak imzalanır ve ardından blok zincir ağına yayınlanır. Dijital imzalı bir kayda, ağdaki tüm katılımcılar tarafından görülebilen açık anahtar (*public key*) bilgisiyle erişilir.

3.3. Uzlaşma Protokolleri ve Sistemin İşleyişi

Dağıtık ortamda, düğümler arasında nasıl fikir birliğine ulaşılır? Blok zincir sisteminin işleyişi kapsamında kullanılacak uzlaşma protokolü (*consensus protocols*) önemli bir konudur. Blok zincir sistemlerinde, birbirine güvenmeyen düğümler arasında nasıl uzlaşmaya varılacağı konusu, Bizans Generalleri (*Byzantine Generals - BG*) probleminin bir dönüşümü olarak ifade edilmektedir (Zheng vd., 2017; Zheng vd., 2018). Blok zincir ağına bulunan düğümler, salt çoğunluğun onayı olmadan, zincire yeni bir kayıt ekleyemez. Bu noktada, düğümlerin ağ üzerinde ortak bir protokol üzerinde anlaşması gerekir; böylece yeni bir kayıt yani veri ekleyip yayınlatabilirler. Blok zincir sistemlerinde, dağıtık olarak düğümlerde bulunan kayıt defterlerinin tutarlı olmasını sağlamak için uzlaşma protokolleri, diğer adıyla uzlaşma algoritmaları (*consensus algorithms*) kullanılmaktadır. Tüm düğümlerin, dağıtık defterlerin mevcut durumu hakkında ortak bir anlaşmaya varmasını sağlayan algoritmadır. Böylece, blok zincir ağına yüksek güvenilirliği sağlar ve dağıtık bir ortamda birbirini tanımayan/güvenmeyen eşler (düğümler) arasında güven ortamı oluşturur (Panarello vd., 2018; Zheng vd., 2018).

Şimdi, blok zincir sisteminin nasıl çalıştığını kısaca inceleyelim. Blok zincir sisteminde pek çok kullanıcı, düğümler üzerinden işlem (para aktarma, veri sahipliğini devretme, ortak bir veriyi güncelleme ve benzeri işlem) talebi gerçekleştirebilir. Bir düğüm bir işlem talebi (örneğin Şekil 4'te para transferi işlem talebi) gerçekleştirdiğinde, dijital imza ve benzeri

kriptografik bileşenlerle beraber içeriği hazırlanır ve ardından bunu blok zincir ağında yayımlar. Oluşturulan kayıt, diğer düğümler üzerinden blok zincir ağına yayılır. Yeni oluşturulan kayıt, farklı düğümler tarafından oluşturulan diğer kayıtlar ile birlikte bir havuzda bekletilir. Kayıtların blok zincir ağına dahil olması için, özel düğümler - diğer adıyla madenci düğümler (*miner nodes*) - tarafından zaman damgalı bir aday blok haline getirilir. Üretilen aday bloğun dağıtık kayıt defterine yani zincire eklenebilmesi için, düğümler arasında uzlaşma protokolü çalışır. Uzlaşma protokolü, bir bulmacadır ve bulmacanın çözümünde mutabakata ulaşırsa aday blok onaylanır. Ardından, bu yeni blok, kayıt defterinin yeni zincir halkası olarak tüm düğümler tarafından zincire eklenir (Fernández-Caramés & Fraga-Lamas, 2018).

Şekil 4. Blockchain Sistemi Nasıl Çalışır?

Günümüzde, blok zincir sistemlerinde çeşitli uzlaşma protokolleri kullanılmaktadır. Nakatomo ilk uzlaşma protokolü olarak karmaşık bulmacaların çözülmesine dayalı *Proof of Work (PoW)* protokolünü sunmuştur. Bunun yanında, *Proof of Stake (PoS)*, *Practical Byzantine Fault Tolerance (PBFT)*, *Delegated Proof of Stake (DPoS)*, *Proof of Bandwidth (PoB)*, *Proof of Elapsed Time (PoET)*, *Proof of Authority (PoA)* gibi başka uzlaşma protokolleri de kullanılmaktadır.

3.4. Blok Zincir Sistemleri

Son olarak, blok zincir sistemlerine ve popüler blok zincir platformlarına kısaca değinmemiz faydalı olacaktır. Belli birtakım mimari özellikleri ve çalışma prensiplerinin yanında, blok zincir sistemleri genel olarak üç gruba ayrılmaktadır (Zheng vd., 2018; Fernández-Caramés & Fraga-Lamas, 2018; Panarello vd., 2018; Tanrıverdi vd., 2019): genel (*public*) blok zincir, özel (*private*) blok zincir ve konsorsiyum (*consortium*) blok zincir.

Genel blok zincir sistemlerinde, dağıtık defter yani tüm kayıtlar halka açıktır. Bu sistem türünün en iyi bilinen örnekleri Bitcoin (<http://bitcoin.org>) ve Ethereum (<http://ethereum.org>)’dur. Açık bir platform olan Genel blok zincir sisteminde herkes ağa katılabilir ve kayıt ekleyebilir; herkes blokları doğrulayabilir. Herhangi bir özel düğüm barındırmamaktadır. Bu sistemlerde, ağa katılmak için herhangi bir kısıtlama yoktur. Bu sebeple izinsiz (*permission-less*) blok zincir olarak da adlandırılır.

Özel blok zincir sistemlerinde ise, bir ağ yöneticisinin daveti veya tanımladığı belli kurallara yeni düğümlerin ağa katıldığı sistemlerdir. Özellikle bir kurum veya organizasyon içerisindeki veri paylaşımı için tercih edilmektedir. Ağa davetli olan düğümlerin uzlaşma sürecine katılmasına izin verilmektedir. Özel bir izni olmayan kişilerin zincire katılması mümkün değildir; bu sebeple izinli (*permissioned*) blok zincir olarak da adlandırılır. İzinli bir yapıya sahip olması, blok zincir teknolojisinin merkezi olmayan yapısına uygunluğunu kısmen azaltmaktadır.

Konsorsiyum blok zincir sistemleri ise, her isteyenin katılabildiği genel blok zincir sistemleri ile bir yöneticinin onayı ile ağa katılımın gerçekleştiği özel blok zincir sistemleri arasında olan bir modeldir. Eşit derecede karar verici bir grubun - doğrulayıcı düğümlerin - bulunduğu sistemlerdir. Ağın herkese açık/sınırlı olmasına ve ağdaki herkesin veri okuma/yazma işlemlerine sahip olma/olmama durumları bu düğümler tarafından belirlenir. Kısmen izinli sistemler olarak adlandırılır. Oluşturulan zincirin görünürlüğü doğrulayıcılarla sınırlı olabilir, yetkili kişilerce görülebilir veya herkes tarafından görülebilir. Konsorsiyum blok zincir sistemi, aynı sektörde birden fazla kuruluşun faaliyet gösterdiği ortamlar için çok faydalıdır. Aynı sektördeki diğer paydaşlarla veri paylaşımı için ortak bir zemin hazırlar.

Günümüzde Ethereum, Hyperledger, Ripple, Quorum, Corda gibi kullanım amaçları, çalışma mantığı ve tasarım bakımından farklılaşan birçok blok zincir platformu bulunmaktadır. Örneğin, Akıllı Sözleşmelerin geliştirilmesini sağlayan en önemli blok zincir platformu Ethereum’dur. Ethereum’u kriptopara olarak kullanmanın ötesinde, merkezi olmayan uygulamaların geliştirilmesine ve çalıştırılmasına da olanak sağlayan Genel blok zincir sınıfından

bir platformdur. Ethereum, kurumsal amaçlı Özel blok zincir ağlarının oluşturulmasında da kullanılmaktadır. IBM tarafından sunulan Hyperledger Fabric (<https://www.hyperledger.org>) platformu ise, farklı endüstriler için blok zincir uygulamaları geliştirmeyi ve özel blok zincir sistemi oluşturmayı sağlayan bir platformdur. Hyperledger platformunun çalışma mantığı, “chaincode” olarak adlandırılan Akıllı Sözleşmelere ve Akıllı Sözleşmelerin çalışmasına olanak sağlayan konteyner (*docker*) teknolojisine dayanır.

3.5. Akıllı Sözleşmeler

Akıllı Sözleşmeler, blok zincir teknolojisinin kriptopara birimlerinin ötesinde kullanılabilirliğinin önemli göstergelerinden biri olmuştur. Blockchain 2.0 olarak bilinen ikinci nesil blok zincir döneminin oluşmasını sağlayan Akıllı Sözleşmeler, teknik bir ifadeyle şu şekilde tanımlanabilir: belli bir dizi olayın yürütülmesi için geliştirilmiş, uzlaşma protokolleri kullanan, ağ üzerinde depolanan ve çalışan, olay odaklı program parçalarıdır. Önceden belirlenen durumların veya olayların oluşması sonucunda, Akıllı Sözleşmelerde tanımlanmış ilgili fonksiyonlar tetiklenir ve sözleşme içeriğindeki komutlar otomatik olarak gerçekleştirilir. Akıllı Sözleşmelerin değiştirilemezliği, tutarlılığı ve şeffaflığı da blok zincir sistemi tarafından sağlanmaktadır.

Akıllı Sözleşmeler, merkezi bir tarafın (banka, noter ve benzeri üçüncü tarafların) kontrolü ve denetimi olmadan, klasik sözleşmelerin dağıtık bir mimari ile uygulanmasıdır. Bu bağlamda Blockchain 3.0 olarak adlandırdığımız üçüncü nesil blok zincir gelişimini de desteklemiştir. Akıllı Sözleşmeler - finans, gayrimenkul, sigorta, tedarik zinciri, sağlık ve benzeri alanlarda - belli durumların izlenerek güvenilir ve otomatik işlemlerin gerçekleştirilmesini ve buna bağlı olarak maliyet, hız ve güvenlik avantajlarının elde edilmesini sağlamaktadır.

Örneğin, uzaktan hasta bakımı kapsamında kronik hastalığa sahip bireylerin evlerinden belli teknolojilerle sağlık durumlarının izlenerek, verilerin blok zincir ağında saklanması; Akıllı Sözleşmeler ile toplanan sağlık verilerinin sonuçlarına göre yapılması gereken işlemlerin otomatik olarak gerçekleştirilmesi sağlanabilir. Benzer şekilde, Akıllı Sözleşmeler sigorta talebi ve geri ödeme süreçlerinin daha hızlı çözülmesini, ilaç tedarik zincirine dair daha şeffaf veriler elde edilmesini ve birçok kullanım durumunu sağlayabilir.

4. Neden Sağlıkta Blok Zincir?

Blok zincir hastaların sağlık verilerinin saklanmasından, ilaç tedarikinde sahteciliğin önlenmesine kadar birçok alanda sağlam ve güvenilir bir altyapı sağlayabilir. Son yıllarda, araştırmacılar blok zincir teknolojisinin bir alanda gerçekten bir ihtiyaç veya çözüm olup ol-

madığı, çözüm olması durumunda hangi türde bir sisteme ihtiyaç olduğu konusunda değerlendirme modelleri veya karar ağaçları kullanmaktadırlar (Fernández-Caramés & Fraga-Lamas, 2018; Mulligan vd., 2018; Peck 2017). Bu değerlendirme yöntemleri, aslında ihtiyaç analizi yapılan -makro düzeyde- bir sektörün veya - mikro düzeyde - bir uygulama alanının, blok zincir sisteminin sahip olduğu yetenekler ve özellikler ile sistematik bir karşılaştırmasına imkan sağlamaktır. Peck (2017) tarafından sunulan karar ağacı model (Şekil 5), yaygın olarak çalışmalarda kullanılan pratik modellerden biridir. Şimdi, bu çerçevede neden sağlıkta blok zincir konusunu özetleyelim.

Geleneksel veritabanı teknolojileri ihtiyacı karşılıyor mu? Sağlık alanındaki güncel gelişmelere ve gereksinimlere baktığımızda, hasta kontrolünde veri yönetiminin sağlandığı modellere ihtiyaç duyulmaktadır. Geleneksel merkezi veritabanı sistemleri, modern teknolojilerle entegrasyonu konusunda artık yetersiz kalmaktadır. Merkezi bir ortamda verilerin depolanması veri güvenliği ve saldırılar açısından risk teşkil etmektedir. Heterojen veri kaynaklarının artışıyla büyük sağlık verilerinin yönetimi, dağıtık ortamlardaki verilerin güvenliği ve sistemler arası birlikte çalışabilirlik sorunlarının karşılanması gerekmektedir.

Birden fazla katılımcının verileri güncelleyebilmesi gerekiyor mu? Sağlık sektörünün doğasında çok sayıda paydaş bulunmaktadır. Sağlık alanındaki her paydaş, sahip oldukları belli birtakım görevleri yerine getirebilmek veya isteklerine ulaşmak amacıyla, belli birtakım verilere erişmeye, verileri güncellemeye ve diğer paydaşlarla veri alışverişine ihtiyaç duyar. Bu işlemlerin kontrollü bir erişim mekanizması ile güvenli bir şekilde gerçekleşmesi de gerekmektedir.

Tüm paydaşlar birbirine güveniyor mu? Sağlık çok geniş bir ekosistem olmakla beraber birçok hassas verinin değişimini barındıran dinamik bir yapıdır. Sağlık alanında her paydaş gerçekleştirdiği işin doğasına bağlı olarak birtakım hassas ve gizli bilgilerin işlenmesiyle meşguldür. Bu kapsamda, sağlık bilgi yönetim sistemleri, sigorta talep sistemleri, sağlık tedarik zinciri sisitemleri, çeşitli siber saldırılar, sahtecilik ve benzeri kötü amaçlı saldırılara maruz kalabilmektedir. Yeni teknolojik çözümlerle, veri paylaşımının şeffaflığına ve paydaşlar arasında güven ortamına ihtiyaç bulunmaktadır.

Şekil 5. Blok Zincir Karar Ağacı (Peck, 2017)

Tüm paydaşların güvendiği bir üçüncü taraf var mı? Dağıtık ekosistem yapısı, merkezi tek bir üçüncü tarafın tüm verileri yönetmesini zorlaştırır. Özellikle hasta merkezli bakım yaklaşımıyla çok sayıda yenilikçi teknolojiler hayatımıza girmiştir ve bu durum kişisel sağlık verilerinin çeşitli ortamlarda depolanması, sağlık verilerinin hareketliliğini ve merkeziyetçilikten uzak bir altyapının verimli yönetilmesi ihtiyacını artırmaktadır. Her paydaşın kendilerine ait verilerinin sahipliğini, yönetimini ve kontrolünü gerçekleştirebilir olması gerekmektedir.

Verilerin gizliliğine ihtiyaç var mı? Blok zincir teknolojisinin en önemli özelliklerinden biri de değiştirilemez kayıtları oluşturmastır. Sağlık alanında da güçlü veri güvenliği ve gizliliği, değiştirilemez veri kayıtlarının oluşturulması oldukça değerlidir. Sağlık verilerinin yok edilemez ve izinsiz kişilerce ele geçirilemez şeklinde korunması gerekmektedir.

Blok zincir sisteminde *kimin değişiklikler yapabileceğinin kontrolüne ihtiyaç var mı?* Sağlıkta oluşturulabilecek bir blok zincir sisteminde, paylaşılacak olan sağlık kayıt defterine (yani veritabanına) erişimi olan ve deftere yazan düğümlerin bilinmesi uygun olacaktır. Herkese açık bir ağ yapısını kullanmak yerine; veri okuma/yazma işlemlerini yapma, blok oluşturabilme, doğrulama yapabilme gibi hakların belli düğümlere tanımlanması, ağın iç işleyişi bakımından hız ve verimlilik sağlayacaktır. Sağlık sektöründe faaliyet gösteren çeşitli tarafların kullanımı için bir *Ulusal Konsorsiyum* Blok Zincir sistemi, elektronik sağlık kayıtlarının yönetimi için güvenilir bir dağıtık depolama ve veri paylaşım imkanı sağlayabilir.

5. Sağlık Alanında Blok Zincir Uygulamaları

Sağlık ekosisteminde blok zincir uygulamaları amaçlarına göre dört ana kategoride incelenmektedir (Şekil 6): sağlık kayıtlarının yönetimi, sağlık tedarik zincir yönetimi, sağlık sigortası süreçlerinin yönetimi, sağlık veri analizleri ve klinik araştırmalar.

Şekil 6. Sağlıkta Blok Zincir Uygulama Alanları

4.1. Sağlık Kayıtlarının Yönetimi

Sağlık kayıtlarının yönetimi, blok zincir teknolojisinin en yaygın uygulama alanlarından biridir. Dünya çapında, sağlık kayıtlarının yönetimi kapsamında çok sayıda blok zincir platformu ve projesi bulunmaktadır; bu uygulama alanında rekabet oldukça yüksektir. Hastanın sağlıkla ilişkili işlem verisi, katılımcılar (aile hekimi, hastaneler, laboratuvarlar ve diğer sağlık hizmeti sağlayıcıları) tarafından oluşturulabilir; hasta hakkında tüm hassas sağlık verileri (kimlik bilgisi, tıbbi öykü, tanı, tedavi, laboratuvar test sonuçları, raporları, reçete bilgileri, doktor bilgileri ve benzeri) güvenli bir şekilde kayıt defterinde depolanabilir; hasta kontrolünde ve izninde paylaşımı gerçekleştirilebilir (HIMSS, 2020; Nguyen vd., 2019; McGhin vd., 2019 Zhang vd., 2018).

Blok zincir altyapısı ile, *HIPAA*, *GDPR* gibi düzenlemelerle uygun olarak, hastalar tarafından açıkça izin verilmedikçe hassas verilerin işlenmesini yasaklayan, hasta kontrolünde verilerinin paylaşıldığı ve yönetildiği *akıllı sağlık profiline* oluşturulması mümkün olmakla beraber, yaygın olarak bu yaklaşım ile uygulamalar geliştirilmektedir. Bu kapsamda önemli bir nokta da, her blok zincir sistemi için temel bir uygulama alanı olan *kimlik yönetimidir*. Blok zincir ağında bulunan tüm katılımcılara (hasta, doktor, hastane, teknisyen ve benzeri) ve hatta akıllı nesnelere ait kimlik bilgilerinin ağ üzerinde doğrulanarak saklanması gerekmektedir. Özellikle e-devlet uygulamalarının da temelini oluşturan bu kullanım durumu, sağlık kayıtlarının yönetimi uygulamalarında da önemli bir yeri vardır.

IoT, akıllı telefonlar, giyilebilir teknolojiler gibi hayatımıza giren çok sayıda katma değerli teknoloji bulunmaktadır. Bu teknolojiler - bahsettiğimiz üzere - kişisel sağlık sistemlerinin gelişimini de oldukça fazla etkilemiştir. Bu teknolojilerle beraber bireyler, çeşitli kaynaklardan toplanan fiziksel aktivite, fitness veya yaşam tarzı verilerini kişisel sağlık uygulamalarında (örneğin Apple Health, Microsoft HealthVault) toplamaktadırlar ve izlemektedirler. Şekil 6'da gösterildiği üzere, bireyler sahip oldukları heterojen sağlık uygulamalarından veya sistemlerinden elde ettikleri kişisel sağlık kayıtlarını blok zincir ağında doğrulanarak depolanmasını sağlayabilir; tüm sağlık verilerini paylaşılan ortak bir kayıt defterinde koruyabilir; ve diğer paydaşlarla bu verilerini kontrollü olarak paylaşabilir.

Şekil 6. Blok Zincir Tabanlı Sağlık Kayıtlarının Yönetimi Kavramsal Modeli

Uzaktan hasta izleme (*remote patient monitoring*), hastanın durumunu geleneksel sağlık ortamları dışında uzaktan, gerçek zamanlı bir şekilde izleyebilmektir. Bu sürecin sağlanması amacıyla Kablosuz Vücut Alan Ağları (*Wireless Body Area Sensor Networks, WBAN*), giyilebilir akıllı IoT cihazları, mobil cihazlar ve benzeri teknolojiler kullanılarak tıbbi verilerin toplanması sağlanmaktadır. Blok zincir teknolojisi, uzaktan toplanan sağlık verilerinin zaman damgalı ve değiştirilemez bir kayıt olarak saklanması, paylaşılması ve izlenebilirliği için de bir araç olabilir. Akıllı Sözleşmelerin etkili kullanımı ile paydaşlar arasında koordinasyon sağlanabilir. Örneğin uzaktan hasta bakımında mobil cihazlardan elde edilen verileri saklama ve Akıllı Sözleşmeler ile otomatik müdahaleler sağlama; acil hizmet sağlayıcıları ile veri paylaşımı gibi katma değerli servislerin sağlanmasına imkan tanır.

Sağlık ekosisteminde aktörler arasında oluşturulabilecek bir blok zincir sağlık ağı, sağlık kayıtlarının yönetimi için güvenli bir altyapıya sahiptir. Akıllı Sözleşmelerin kullanılmasıyla, kullanıcılar için kimlik yönetimiyle entegre bir *akıllı sağlık profili* oluşturabilir. Yine, Akıllı Sözleşmeler ile erişim kontrolü ve rol tabanlı ayrıcalıkların altyapısı geliştirilebilir; sağlık kayıtlarının hasta tarafından yönetimi de sağlanabilir. Hem veri kaynağının hem de veri erişim geçmişinin (hangi sağlayıcının, ne zaman ve hangi veriyi kullandığı bilgilerinin) ağ üzerinde değişmez denetim günlükleri (*immutable audit logs*) kullanıcılara şeffaflık sağlayacaktır. Tablo 2’de bu kategoriye ait bazı uygulama örnekleri paylaşılmaktadır.

Tablo 2. Sağlık Verilerinin Yönetimi Kapsamında Blok Zincir Uygulamalarına Örnekler	
Uygulama	Açıklama
MedRec	MIT Media Lab tarafından, sağlık verilerine erişimi kolaylaştırmak ve iyileştirmek amacıyla geliştirilmiş bir <i>Ethereum Blockchain</i> sistemidir. MedRec, hastanın tüm bilgilerini tek bir yerde saklayarak hastaların ve doktorların bu verileri şeffaf bir şekilde görüntülemesini kolaylaştırır. Kaynak: https://medrec.media.mit.edu
phrOS	Taipei Medical University Hospital ve Digital Treasury Corporation (DTCO) tarafından sunulan hastaneler genelinde bir blok zincir entegrasyon projesidir. Hastanın tüm tıbbi bilgilerini ve görüntü verilerini blok zincir ağına ekleyerek sağlık sektöründeki işbirliğini hızlandırmayı ve şeffaflığı artırmayı hedefler. Doktorlar ve hastalar tarafından mobil uygulama üzerinden erişilebilir. Kaynak: https://phros.io
MTBC	Hastalara sağlık kayıtları üzerinde tam kontrol sağlayan, heterojen sistemler arasında birlikte çalışabilirlik sağlayan, ve hasta kontrolünde veri yönetimi imkanı sunan, Hyperledger platformunda geliştirilmiş bir blok zincir sistemidir. Kaynak: https://www.mtbc.com
HashedHealth	Sağlık sektöründeki profesyonellerin kimlik bilgilerini daha şeffaf ve kolay erişilebilir hale getirmeyi amaçlayan bir blok zincir sistemidir. Profesyonel Kimlik Bilgisi Değişimi ile, kullanıcılar çeşitli sağlık profesyonellerinin kimlik bilgilerini doğrulayabilir ve kayıtlarını izleyebilir. Sağlık profesyonellerinin, işe alım sürecini kolaylaştırır ve aynı zamanda bir profesyonelin sağlık kariyer geçmişinin değiştirilemez bir kaydını inceleyebilir. Kaynak: https://hashedhealth.com
Medicalchain	Elektronik sağlık kayıtlarının hastalar tarafından tam kontrolünü sağlayan ve bu verileri güvenli bir şekilde saklayan bir <i>Hyperledger Blockchain</i> sistemidir. Doktorlar, hastaneler, laboratuvarlar, eczacılar ve sağlık sigortacıları gibi farklı kuruluşlar, bir hastanın kaydına erişmek için izin isteyebilir. Hasta ve doktor etkileşimi geliştirmek amacıyla, doktorlarla çevrimiçi iletişime ve teletıp hizmetine imkan sağlıyor. Ek olarak, hastalar ödemelerini kriptoparalarla ya da Medicalchain'in kendi dijital parası olan MedTokens ile yapabilir. Kaynak: https://medicalchain.com
KSI Blockchain	KSI Blockchain (Guardtime Health), Guardtime firmasının desteğiyle Estonya'da tasarlanmış ve e-devlet altyapısında çeşitli hizmetleri sağlamak için kullanılan yüksek güvenlilıklı ulusal bir blok zincir teknolojisidir. Önemli bir ulusal blok zincir ağı örneğidir. Bu sistemde, Estonya vatandaşlarının kimlik bilgileri ve sağlık kayıtlarını güvence altına alınmaktadır. Estonya'nın farklı sağlık hizmeti sağlayıcılarından gelen veriler bu platformda entegre edilmektedir; tüm paydaşlar arasında güvenli ve şeffaf veri değişimi sağlar. Kaynak: https://guardtime.com/health , https://e-estonia.com
SOLVE	Solve.Care Vakfı, sağlık hizmetleri ve diğer fayda sağlayıcı programların küresel olarak dağıtık yönetimini tanımlama misyonuyla kurulmuştur. Bir Ethereum blok zincir ağı olan SOLVE platformu, sağlık ve bakım hizmetlerine erişimi iyileştirme, sağlık hizmetlerinin daha verimli yönetilmesi, sonuçlar için doğru ve zamanında sağlık hizmeti sağlayıcılarına ödeme yapmayı ve maliyetleri azaltmayı amaçlamaktadır. Kaynak: https://solve.care
MediBloc	MediBloc, hastalara, sağlık hizmeti sağlayıcılarına ve araştırmacılara dağıtık bir sağlık bilgi ekosistemi sunar. Hastalar sağlık verilerine daha kolay erişim sağlar ve sağlık hizmeti sağlayıcıları ile bu bilgileri paylaşır. Aynı zamanda, sağlık verilerini araştırmacılara MED Token ile satışını yapabilir. Kaynak: https://medibloc.org/en
Dentacoin	Dentacoin, diş sağlığı sektörü için tasarlanmış ilk blok zincir sistemidir. <i>Ethereum</i> tabanlı olan bu ağ, diş hekimleri ve hastalar arasında güvenli bir etkileşim oluşturmaktadır. Hasta merkezli diş bakımı, evde uygun diş bakımı alışkanlıklarının kazandırılması konusunda hatırlatmalar, bildirimler, tavsiyeler ve akıllı tedavi servisleri sunmaktadır. Kaynak: https://dentacoin.com

Lympo (LYM)	Lympo, <i>Ethereum Blockchain</i> teknolojisini kullanan bir kişisel sağlık cüzdanı platformudur. Çok sayıda paydaşı bağlayarak sağlıklı bir yaşam tarzı ekosistemi yaratılması hedeflenmiştir. Sağlık uygulamaları ve giyilebilir cihazlarla üretilen spor ve fiziksel aktivite verilerinin blok zincir ağında toplanarak, daha sağlıklı bir yaşam tarzının geliştirilmesi için kullanıcılara öneriler, hizmetler ve hatta LYM Token teşvikleri ve para kazanma ödülleri sunmaktadır. Kaynak: https://lympo.com
-------------	--

4.2. Sağlık Tedarik Zinciri Yönetimi

Sağlık alanında diğer önemli bir uygulama alanı ise, sağlık tedarik zinciri yönetimidir. Sağlık, ilaç ve tıbbi malzeme endüstrinde tedarik zinciri operasyonlarının verimliliği ve maliyetlerin optimizasyonu önemli hedeflerdir. Bu hedeflere ulaşılabilmesi için tedarik zinciri süreçlerinde güvenilir, zamanında ve şeffaf bilgi akışının sağlanması gerekmektedir. Ürün güvenliği, ürün kaynaklarının takibi, ürün hasarının veya kaybının tespiti, ürün kalite kontrol parametreleri, sıcaklık ve benzeri gerekliliklere uygunluğu gibi konularda verilere ihtiyaç vardır. Veri toplama ve analizi kapsamında RFID (Radyo Frekansı ile Tanımlama, *Radio Frequency Identification*), IoT, WSN, hücresel ağ gibi teknolojiler önemli avantajlar getirmiştir.

Günümüzde, sağlık tedarik zincirinin karmaşık olan doğasını doğru bilgi akışı ile iyileştirmek; şeffaflık ve operasyonel verimlilik kazandırmak; karar verme süreçlerini güçlendirmek; hatta tam zamanında (*just-in-time*, JIT) stratejileri desteklemek amacıyla blok zincir teknolojisi uygulanmaya başlanmıştır (Şekil 7). Hatta bu kapsamda dünya çapında sadece sağlık değil, diğer birçok tedarik zinciri yapısında önemli yatırımlar ve girişimler bulunmaktadır. Blok zincir teknolojisi, tedarik zinciri paydaşları arasında azalan güveni iyileştirmek, veri bütünlüğünü ve şeffaflığı sağlamak için güçlü bir araç olarak görülmektedir (HIMSS, 2020).

Şekil 7. Blok Zincir Tabanlı Sağlık Tedarik Zinciri Kavramsal Modeli

Sağlık alanında özellikle sahtecilikle mücadele konusunda yoğun çalışmalar bulunmaktadır. Blok zincir ağında ilaç, reçete, tıbbi cihazlar ve benzeri ürünlere ait işlemlerin ve para transferi işlemlerinin değiştirilemez kayıtlarla izlenebilirliği sağlanabilir. Bilindiği üzere sahte veya standart dışı ilaçların kullanımı, hastalar için çok ciddi sonuçları doğurabilir. Bu durum, dünya çapında ilaç endüstrisinde karşılaşılan yaygın bir sorundur. Sağlık ekosisteminde bulunan tüm paydaşların bağlı olduğu blok zincir ağında kayıtlı bulunan ilaçların reçetelenmesi ile ilgili her işlemin kaydı sağlanabilir. Bu şekilde, taraflardan herhangi biri tarafından reçetede yapılabilecek bir değişiklik tespit edilebilir. Paylaşılan kayıt defteri yapısı ve denetlenebilirlik, reçete izlemeye sadece reçeteleri daha güvenli hale getirmekle kalmayıp, aynı zamanda daha az reçete yazma konusunda teşvik edici bir yaklaşım da sağlayabilir. Tablo 3'te sağlık tedarik zinciri uygulamaları kapsamında bazı uygulama örnekleri paylaşılmaktadır.

Tablo 3. Sağlık Tedarik Zinciri Kapsamında blok zincir Uygulamalarına Örnekler	
Uygulama	Açıklama
FarmaTrust	Sahte ilaçları ortadan kaldıran, ilaç tedarik zincirleri için verimlilik sağlayan ve ilaçların çevrimiçi olarak satın alınmasına izin veren bir <i>Ethereum Blockchain</i> sistemidir. Aynı zamanda yapay zeka teknolojilerini ve büyük veri analizi kullanır. Kaynak: https://www.farmatrust.com
MediLedger	İlaç tedarik sürecinin güvenliğini ve takibini sağlamak ve uyuşturucu kaçakçılığı, sahte ilaçlar gibi şüpheli ve kötü niyetli etkinlikleri tespit etmek amacıyla geliştirilmiş bir blok zincir sistemidir. İlaç üreticileri ve distribütörlerini bir araya getirerek ilaçların yapıldığı hammaddelerin doğrulanmasına ve sahte ürünlerin hemen tespit edilmesine yardımcı olur. Kaynak: https://www.mediledger.com ; https://www.chronicled.com
iSolve - ADLT	ADLT (Advanced DLT), kurumsal bir blok zincir platform çözümdür. Güvenilir ilaç tedarik zincirinin oluşturulmasını sağlamak için bir paydaştan diğerine ilaçların hareketini izler; ilaç tedarik zincirini şeffaf hale getirir. Küresel mevzuata uygunluk, gelişmiş stok kontrolü ve yönetimini sağlar; sahte ilaçların tedarik zincirine girmesini önler; paydaşlar arasında güvenli iletişim sağlar. Kaynak: https://isolve.io
Synthium Health	Üreticiler, distribütörler, sağlık hizmeti sağlayıcılar ve diğer katılımcılara yardımcı olmak için Synthium, tedarik zinciri ağında kaynak kullanımından dağıtımına kadar tüm işlemleri korumak, güncellemek ve izlemek için şeffaf ve verimli bir <i>Ethereum Blockchain</i> platformu sağlar. İsteğe bağlı raporlamaya olanak tanır. Kaynak: https://www.synthiumhealth.com

4.3. Sağlık Sigorta Süreçlerinin Yönetimi

Sağlık sigortası talep işleme ve geri ödeme süreçleri, poliçe sahipleri (yani hastalar) için karmaşık ve kimi zaman uzun süren süreçler olabilmektedir. Temel amaç, sağlık kuruluşları, sağlık sigortası firmaları ve poliçe sahipleri arasındaki etkileşimin optimize edilmesi, süreçlerin hızlandırılması, kullanıcı odaklı ve kullanıcı dostu bir yöntem uygulanmasıdır. Sağlık hizmetlerinde blok zincir altyapısı ile elde edilecek güvenilir sağlık kayıtlarının yönetimi, aynı zamanda daha verimli, hatasız ve şeffaf sigorta süreçlerini de sağlayacaktır (Kuo vd., 2017; Zhang vd., 2018; McGhin vd., 2019).

Blok zincir teknolojisi ile sağlık kayıtları ve buna bağlı sigorta talep yeterliliği işlemleri doğrulanabilir; hızlı ve verimli işlenmesi sağlanabilir. Böylece şeffaf ve doğru kararların alınması kolaylaştırabilir; geri ödeme işlemlerinin, ön ödemelerin veya alternatif ödeme süreçlerinin hızlandırılmasını, otomatik hak taleplerinin sağlanmasını ve finansal süreçlerin iyileştirilmesini sağlayabilir. Özellikle, Akıllı Sözleşmelerin kullanımı sigorta süreçlerinin yönetimini geliştirir. Yetkili taraflarca alınan sağlık hizmetleri, sağlık hizmetinde kullanılan tıbbi ürünler ve benzeri verilere erişebilirlik sağlanır. Bu durum aynı zamanda talep süreçlerinin denetimini ve sahtekarlık tespitini kolaylaştırır. Bu alanda uygulama örnekleri özellikle finans uygulamalarıyla entegre gelişmektedir. Tablo 4'te sağlık alanında bulunan mevcut uygulama örnekleri paylaşılmaktadır.

Tablo 4. Sağlık Sigorta Süreçlerinin Yönetimi Kapsamında Blok Zincir Uygulamalarına Örnekler	
Uygulama	Açıklama
SafeInsure	SafeInsure, sağlık sigorta poliçesi alıcılarına dünya çapında adil fiyat keşfi ve erişim sağlayan dağıtık bir sigorta piyasasıdır. Dürüst ve hesap verebilir bir sigorta pazarı sağlar. Kişisel sigorta taleplerinin çeşitli sağlayıcılara iletilmesini ve uygun sigorta tekliflerine erişimi sağlar; sahtekarlığı engeller. Kaynak: https://www.safeinsure.io
PokitDok	PokitDok, gerçek zamanlı sağlık sigortası uygunluk doğrulaması sağlayan bir blok zincir çözümdür. Sigorta taleplerinin hızlı ve kolay bir şekilde iyileştirilmesini sağlar; verimsiz süreçleri azaltır ve gerçek zamanlı sağlık sigortası kontrolleri sağlamaktadır. Kaynak: https://pokitdok.com

4.4. Sağlık Veri Analizleri ve Klinik Araştırmalar

Sağlık araştırmacıları tarafından hastalıklara ait tedavi modellerinin geliştirilmesi, önlenmesi, semptomların teşhisi ve hafifletilmesi, yeni ilaçların keşfi, ilaç uygunluğunun araştırılması, tıbbi cihazların tedavi sürecindeki etkinliğinin araştırılması, salgın hastalıkların erken tespiti gibi çeşitli amaçlarla klinik araştırmalar ve sağlık veri analizleri gerçekleştirilmektedir. Blok zincir teknolojisinin sağlık alanındaki diğer önemli bir uygulama alanı ise dağıtık kayıt defterinde bulunan sağlık verilerinin klinik araştırmaları ilerletmek için kullanılmasıdır (Kuo vd., 2017; McGhin vd., 2019; HIMSS, 2020). Blok zincir altyapısında bulunan (tıbbi öykü, tanı, tedavi, DNA kayıtları, yaşam tarzı, fiziksel aktivite gibi) büyük verilerin makine öğrenmesi, derin öğrenme, yapay zeka ve benzeri algoritmalarla çalıştırılması ve özel sağlık korunması, önleyici tıp ve halk sağlığı yararına kullanılması mümkündür.

Günümüzde blok zincir tabanlı sağlık veri paylaşım ağlarında bulunan verilerin, klinik araştırmalar için geliştirilmesi ve yaygınlaştırılması konusunda çalışmalar yapılmaktadır. Tablo 5'te klinik araştırmalar amacıyla geliştirilmiş örnek blok zincir platformları paylaşılmıştır. Özellikle genom dizilerinin, DNA kayıtlarının klinik araştırmalarda kullanılması kapsamında blok zincir uygulamaları oldukça popülerdir. Katılımcıları teşvik etmek amacıyla, kişisel sağlık bilgilerinden para kazanmayı sağlamaktadır.

Tablo 5. Sağlık Sigorta Süreçlerinin Yönetimi Kapsamında Blok Zincir Uygulamalarına Örnekler	
Uygulama	Açıklama
Nebula Genomics	Nebula Genomics, kişinin blok zincir teknolojisini kullanarak, kendi genom dizisine sahip olmasını sağlar. Genom dizisinin çıkarılmasında ve çıkarılan genom dizisinin klinik araştırmalarda kullanılması için satılmasında Nebula'nın oluşturduğu kriptopara kullanılır. Genoom dizisi sahibi gizli kalmaktadır ve çıkarılan genom dizisinin kime ait olduğu, kişinin kendisi haricindeki kimse tarafından bilinmemektedir. Genom dizisinden yararlanılarak tanılar daha kolay konulması, hastalıkların önlenmesi, kişiye özel ilaçların geliştirilmesi yaygınlaşacaktır. Kaynak: https://nebula.org/
Genome Chain	Genome Chain (GNC), herkesin kendi genom verilerini kullanarak yaşam tarzını yönetmesini veya geliştirmesini sağlayan DNA tabanlı açık paylaşım ekosistemi sunar. Paylaşılan ekonomi ekosistemi, tıp ve bilim teknolojilerindeki ilerlemeleri hızlandırmak için kullanılır. Bireyler, genom verileri her kullanıldığında ödüllendirilecek ve genom verilerinin rızası olmadan kötüye kullanılmayacağına veya erişilmeyeceğinden emin olur. Kaynak: http://genecoin.me
EncrypGen	EncrypGen (Gene-Chain), genomik tanımlanmış hassas verilerin güvenli bir şekilde paylaşımı ve bilimsel araştırmacılara ve laboratuvarlara bu verilerin satılması amacıyla oluşturulmuş bir blok zincir platformudur. DNA test sonuçlarının, klinik araştırmalarda kullanılarak hastalıklar için daha iyi tedavi yöntemlerinin bulunması için kullanılır. Kaynak: https://encrypgen.com
MedicCoin	MedicCoin, bilimsel araştırmalara ve hayır kurumlarına bağışlarda bulunarak insanlığa fayda sağlamayı amaçlayan bir blok zincir platformudur. Bilim insanlarına diyabet, MLS, Alzheimer, gibi birçok hastalığın tedavisinin araştırmalarına yardımcı olur. Kaynak: https://mediccoin.com
Humanscape	Humanscape, dünyadaki birçok tedavi edilemeyen hastalıkla başa çıkmak ve gerekli tedavileri geliştirmek amacıyla oluşturulmuş bir sağlık hizmeti veri paylaşım <i>Ethereum Blockchain</i> platformudur. Kaynak: https://www.humanscape.io
InnovativeBioresearchClassic	Innovative Bioresearch şirketi HIV, kanser ve rejenerasyon araştırmaları alanında yenilik getirmek amacıyla kurulmuştur. InnovativeBioresearchClassic, bir <i>Ethereum Blockchain</i> sistemidir. Bu sistemde, bir ödeme aracı olarak INNBC Token'ı yeni AIDS tedavisi araştırmalarını geliştirmek amacıyla kullanılır. Kaynak: https://www.innovativebioresearch.com/innbc

Blok zincir teknolojisi, dağıtık veritabanında bulunan - kullanımına izin verilen - sağlık verilerinin anonimleştirilmesini sağlayarak verilerin klinik araştırmalarda kullanılmasını kolaylaştırır. *Veri gizliliğine* ek olarak, veri değişmezliği ilkesiyle, klinik araştırmalar için toplanan *verilerin bütünlüğünü* korumaya devam eder. Diğer önemli bir fayda, klinik çalışmalarda elde edilen sonuçların ve bulguların blok zincir ağında zaman damgası ile izlenebilir, *şeffaf kayıtlara* dönüştürülmesidir. Böylece verilerin yok edilmesi, araştırma sonuçlarının eksik raporlanması veya bazı bulguların hariç tutulması gibi etik dışı davranışların engellenmesini sağlar.

6. Blok Zincirin Yaygınlaşmasında Önemli Konular

Blok zincir teknolojisi kendine özgü tasarım unsurlarına bağlı olarak, doğal olarak bazı kısıtlamalara da sahiptir. Söz konusu kısıtlamaların geliştirilmesi ve iyileştirilmesi konusunda çalışmalar yapılmaktadır. Ernst&Young (2016) tarafından hazırlanan “*Blockchain in Health*” raporunda sağlık alanında önemli dört konunun çözümlenmesi vurgulanmaktadır: Zincir üzeri ve zincir dışı veriler (*on-chain and off-chain data*), ölçeklenebilirlik (*scalability*), teknoloji standartları (*technology standards*), ara katman yazılımları ve uygulama katmanları (*middleware and application layers*)

Zincir üzeri ve zincir dışı veriler: Bilindiği üzere blok zincir teknolojisi, dağıtık mimari yapısına bağlı olarak dağıtık defterin bir kopyasını tüm düğümler ile paylaşmaktadır. Veri işlemlerinin çok yoğun olduğu blok zincir ağlarını düşündüğümüz de, büyük miktarda veriyi içeren bu dağıtık kayıt defteri yani veritabanını, zincir üzerinde saklamak hem gereksiz miktarda veri depolamaya hem de verimsiz bir duruma yol açabilir. Bu kapsamda, verimli zincir dışında (*off-chain*) depolama ve bu veri depolarına güvenli kimlik yönetimi ve izin yapısı ile erişim sağlama yöntemleri üzerinde çalışmalar yapılmaktadır.

Ölçeklenebilirlik: 2009 yılından beri blok zincir endüstrisi muazzam bir dinamizm ile büyümektedir. Blok zincir ağları üzerindeki işlemler, her yıl büyük hızla artmaktadır. Mevcut sağlık sistemlerine ait protokoller, hız ve hacim gerekliliklerini karşılama konusunda birtakım endişeleri de beraberinde getirebilir. Blok zincir sistemlerinde işlem hızı konusu, mutabakat sürecine, yani uzlaşma algoritmasının hesaplamasına bağlıdır. Şu an günümüzdeki uzlaşma algoritmaları ve güvenlik mekanizmalarıyla, bir sağlık veri dosyasının transfer işlemi belli bir zaman alabilir. Sürekli gelişen ve büyüyen dağıtık bir sağlık ağında ölçeklenebilirlik ve daha verimli uzlaşma protokollerini kullanımı konusu önemli bir gereksinimdir.

Teknoloji standartları: Mevcut blok zincir ekosisteminde kendine özel yazılım ve uygulama geliştirme paketlerine sahip Bitcoin, Ethereum, Hyperledger gibi birçok rakip protokol ve platform bulunmaktadır. Farklı protokoller ve test ortamlarının da sağlık sektörüne yararı olacağı açıktır; fakat sağlık alanında blok zincir tabanlı uygulamaları ulusal anlamda daha yaygın ve ölçeklenebilir bir şekilde adapte edilebilmesi için, bazı teknoloji standartlarının geliştirilmesi, düzenlemelerin ve denetim mekanizmalarının belirlenmesi gerekmektedir. Teknoloji standartlarının oluşması, diğer taraftan paydaşlar için yüksek ön maliyetlerin optimize edilmesini de sağlayacaktır.

Ara katman yazılımları ve uygulamalar: Blok zincir teknolojisi, Internet’in altyapısını oluşturan protokoller TCP/IP, DNS gibi bir altyapı teknolojisidir. Blok zincir altyapısı üye-

rinde oluşturulacak ara katman yazılımları ve son kullanıcılara yönelik dağıtık uygulamaların geliştirilmesi önemlidir. Şu an günümüzde çeşitli alanlarda farklı uygulama örnekleri ve girişimler bulunmaktadır; ancak standartlar ve düzenlemelerle blok zincir tabanlı ulusal bir sağlık ağının yaratılması için sağlam düzenlemelere ve standartlara ihtiyaç vardır.

7. Sonuç

Sağlık alanında, noter kaydı gücünde veriler önemli bir gereksinimdir. Hassas sağlık verileri, siber saldırılar için de birincil hedefdir. Tüm sağlık verilerinin güvenli bir şekilde saklanması ve paylaşımı önemlidir. Günümüzde, heterojen veri kaynaklarının arttığı, birlikte çalışabilirliğin önemli bir gereksinim olduğu ve paydaşlar arası güven eksikliklerinin olduğu sağlık ekosisteminde, blok zincir teknolojisi umut verici bir altyapı ve çözüm imkanı sağlamaktadır. Bu bölümde, sağlık alanında mevcut gereksinimlerin karşılanması; ve bireyler, sağlık hizmeti sağlayıcıları, sigorta firmaları, ilaç şirketleri, eczaneler ve diğer aktörler arasında verilerin güvenli bir şekilde paylaşılması konularında blok zincir teknolojisinin potansiyelinden ve güncel uygulama alanlarından bahsedilmiştir.

Blok zincir sistemi üzerinde gerçekleştirilmek istenen bir işlem, ağdaki katılımcıların çoğunluğunun işlemi geçerli kabul etmesi ve uzlaşmaya varması ile - tüm katılımcılarla paylaşılan - dağıtık kayıt defterine eklenir. Paylaşılan veritabanındaki değişiklikler, tüm düğümlerdeki kopyalarına dakikalar veya bazen saniyeler içinde yansıtılır; yani değiştirilmez kayıtların güvenle oluşturulması sağlanır. Sağlık ekosistemindeki tüm aktörlerin, düğümler olarak blok zincir altyapısında bir araya gelmesi; yüksek güvenli verilerin oluşturulması, veri bütünlüğünün ve veri ispatlanabilirliğinin sağlanması demektir.

Mevcut durumda, sağlık alanında blok zincir uygulama örnekleri dört farklı kategori altında gelişmektedir: sağlık verilerinin yönetimi, sağlık tedarik zinciri yönetimi, sağlık sigorta süreçlerinin yönetimi, sağlık veri analizleri ve klinik araştırmalar. Özellikle Akıllı Sözleşmelerle bir blok zincir ağında çok sayıda kullanım durumunu hayata geçirmek mümkündür. Sağlık kayıtlarının doğrulanabilirliği, acil durumların tespiti ve hastaya en doğru müdahalenin yapılması, ilaç reçetelerinin takibi, tıbbi kayıt değişimi ve sahtecilikle mücadele, ilaç veya tıbbi cihaz tedariki faaliyetlerinin izlenebilirliği, sigorta geri ödeme süreçlerinin denetimi, sağlık verilerinin halk sağlığı için anonimleştirilerek klinik araştırmalarda kullanımı gibi birçok uygulama ve proje desteklenmektedir. Aynı zamanda IoT, giyilebilir teknolojiler, kablosuz algılayıcı ağlar, mobil teknolojiler, akıllı cihazlar, yapay zeka, veri analitiği, derin öğrenme ve benzeri modern teknolojilerin gücünü kullanmak için de blok zincir teknolojisi eşsiz bir fırsat sunmaktadır.

Blok zincir teknolojisi ile yeni bir ekonomi modeli gelişmeye devam ederken, diğer yandan birtakım teknik konuların ve kısıtların çözümlenmesi daha sağlıklı bir gelişim süreci sağlayacaktır. Özellikle ülkelerde blok zincir teknolojisi kullanım çerçevesinin teknolojik standartlar ve yasal düzenlemeler ile belirlenmesi, teknolojinin sektörlerde ve çeşitli iş alanlarında yaygınlaşma sürecini kolaylaştıracaktır.

Kaynakça / References

- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, June). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, No. 2, p. 56). Multidisciplinary Digital Publishing Institute.
- Atabaş, H. (2018). Blok Zinciri Teknolojisi. Ceres Yayınları.
- User, E. & User A.S. (2019). Blok Zinciri: Yeni bir Ekonomi Modeli. Cinius Yayınları.
- Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer*, 51(2), 54-58
- Burgess, K., & Colangelo, J. (2015). The promise of bitcoin and the blockchain. *Consumers' Research*: Washington, DC, USA.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654. doi:10.1109/tit.1976.1055638
- Ernst & Young (2016). Blockchain in Health. <https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf>.
- Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6, 32979-33001.
- Gupta, S. S. (2017). Blockchain. John Wiley & Sons, Inc.
- HIMSS (2020). Interoperability in the Healthcare Ecosystem. <https://www.himss.org/what-interoperability>
- Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, 10(10), 470.
- Kuo, T. T., Kim, H. E., & 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.
- McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*.
- Mulligan, C., Scott, J. Z., Warren, S., & Rangaswami, J. P. (2018). Blockchain beyond the hype: A practical framework for business leaders. In *World Economic Forum, White Paper*.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-Health systems. *IEEE access*, 7, 66792-66806.
- Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. *Sensors*, 18(8), 2575.
- Peck, M. (2017). Do You Need a Blockchain? <https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain>
- Sağlık Bakanlığı (2014). EHR (Electronic Health Record) - ESK (Elektronik Sağlık Kaydı). <https://dijitalhastane.saglik.gov.tr>
- Sağlık Bakanlığı (2015). Sağlıkta Birlikte Çalışabilirlik ve Standartlar. <https://dosyamerkez.saglik.gov.tr/Eklen-ti/2840,saglikta-birlikte-calisabilirlik-ve-standartlarpdf.pdf?0>
- Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 463-467). IEEE.

- Swan, M. (2015). Blockchain: Blueprint for a new economy. “O’Reilly Media, Inc.”
- Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217.
- Tübitak Bilgem (2020). Blokzincir. <https://blokzincir.bilgem.tubitak.gov.tr>
- Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, 127, 43-58.
- Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. *Advances in computers* (Vol. 111, pp. 1-41). Elsevier.
- Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017, October). Metrics for assessing blockchain-based healthcare decentralized apps. In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-4). IEEE.
- Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375.
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.