T.C.
MALATYA TURGUT ÖZAL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOK ZİNCİRİ VE SAĞLIK UYGULAMALARI

HAMİT MIZRAK

YÜKSEK LİSANS TEZİ

ENFORMATİK ANABİLİM DALI

EYLÜL -2023

ONUR SÖZÜ

Yüksek Lisans Tezi olarak “Blok Zinciri Ve Sağlık Uygulamaları” başlıklı bu çalışmanın bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım bütün kaynakların, hem metin içinde hem de kaynakçada yöntemine uygun biçimde gösterilenlerden oluştuğunu belirtir, bunu onurumla doğrularım.

Hamit MIZRAK

ÖZET

Yüksek Lisans Tezi

BLOK ZİNCİRİ VE SAĞLIK UYGULAMALARI

Hamit MIZRAK

Malatya Turgut Özal Üniversitesi
Lisansüstü Eğitim Enstitüsü
Enformatik Anabilim Dalı

38 + ix sayfa

2023

Danışman: Dr. Öğr. Üyesi Serpil ASLAN

Dünyada birçok işlemler artık dijitalleştiğinden veri güvenliliği, veri paylaşımı, veriye hızlı erişim ve veri bütünlüğünü korumak son derece önemli görülmektedir. Her geçen gün, günlük yaşantıda bilgisayara olan bağımlılık ve bu bağlılığa paralel olarak yeni verilerin dijital ortamlarda verilerin katlanarak artmasından bahsedilmektedir. Oluşan bu verilerin güvenli bir şekilde paylaşımını sağlamak her geçen gün önemi artmaktadır. Bu verilerin güvenliliğini korumak, muhafaza etmek son derece önem arz etmektedir. Veri güvenliliği konusunda son yıllarda blok zinciri kelimesi sıkça duyulmaktadır. Blok zinciri, güvenli veri paylaşımını, veri bütünlüğünü korumakla görevli, merkezi olmayan dijital kayıt defteri olarak tanımlanmaktadır. Blok zinciri verileri tek yönlü olarak kaydeden, tersine mühendisliğin imkânsız olan ve paylaşımlarını şeffaflık ilkesine göre veri aktarımını gerçekleştirmektedir. Blok zinciri, kaydedilen bu verilerin ortak veri paylaşımına olanak sağlayan, veri güvenliliği korumakla görevli veriye ulaşım süresini kısaltan teknolojinin genel adı olduğu söylenmektedir. Hastaların tıbbi kayıt bilgilerin çalınması, değiştirilmesi hastaların mahremiyeti için çeşitli riskler doğurmaktadır. Bu bilgilerin kötü amaçlı kişilerin vereceği zarar hem hastaya hem de finanse eden kuruma ciddi zararlar vermektedir. Bundan dolayı bulut tabanlı ESK (elektronik sağlık kayıtları), birçok sağlık alanında odak noktası haline gelmektedir. Hasta verilerinin saklanmasında, veri doğruluğunu sağlamada, veri gizliliğini korumakta ve veriyi bulut sisteminde hızlı iletilmesi sağlamak, sağlık sektöründe önemli bir endişe kaynağı haline gelmektedir. Bu tezde, ESK kayıtları için veri erişim kontrolü ve denetimi sağlarken, bulut servis sağlayıcıları yardımıyla sağlık verilerinin paylaşılması için blok zincire ek olarak katmanlı mimari yapısına da değinilmektedir. Bu katmanlı mimari sisteme giriş için, JWT (json web token), hasta bilgilerini özet fonksiyonu (hashing) uygulayarak destekleyici yeni ek çözümler önerilmektedir. Önerilen bu yöntemle, hastanın sağlık kayıtlarını, elektronik ortamda yönetilmesinde ve kontrol edilmesinde kullanılmaktadır. Bu nedenle, blok zinciri platformunda kullanılan bu teknolojilerle daha güvenli sürdürülebilinir yeni kapılar aralamaktadır.

ANAHTAR KELİMELER: Blok Zinciri, Elektronik Sağlık Kayıtları, Özet Fonksiyonu, Bulut Teknolojisi, Akıllı Sözleşme, Veri Tabanı

ABSTRACT

M.Sc. Thesis

BLOCK CHAIN AND HEALTH APPLICATIONS

Hamit MIZRAK

Malatya Turgut Ozal University
Institute of Graduate Studies
Department of Informatics

38 + ix pages

2023

Supervisor: Dr. Instructor Member Serpil ASLAN

Since many transactions in the world are now digitalized, data security, data sharing, fast access to data and maintaining data integrity are considered extremely important. With each passing day, it is mentioned that the dependency on computers in daily life and parallel to this dependency, the data increase exponentially in digital media. The importance of ensuring the secure sharing of this data is increasing day by day. It is extremely important to protect and preserve the security of this data. In recent years, the word blockchain has been heard frequently in terms of data security. Blockchain is defined as a decentralized digital ledger tasked with maintaining secure data sharing and data integrity. Blockchain realizes data transfer according to the principle of transparency, which records data unidirectionally, which is impossible to reverse engineering, and whose sharing is transparent. It is said that the blockchain is the general name of the technology that enables the common data sharing of these recorded data and shortens the time to reach the data responsible for protecting data security. Theft and alteration of patients' medical record information poses various risks to the privacy of patients. The harm that this information will cause by malicious people causes serious harm to both the patient and the financing institution. Therefore, cloud-based EHR (electronic health records) is becoming a focal point in many healthcare fields. Storing patient data, ensuring data accuracy, protecting data confidentiality, and providing fast transmission of data in the cloud system is becoming a major concern in the healthcare industry. In this thesis, while providing data access control and control for EHR records, layered architecture in addition to blockchain is also discussed for sharing health data with the help of cloud service providers. In order to enter this layered architectural system, JWT (json web token), patient information hashing function, supporting new additional solutions are proposed. With this proposed method, it is used to manage and control the patient's health records electronically. Therefore, with these technologies used in the blockchain platform, more secure and sustainable new doors are opened.

KEYWORDS: Blockchain, Electronic Health Record, Summary Function, Cloud Technology, Smart Contract, Database

TEŞEKKÜR

Yüksek lisans tezimin hazırlanma süresince bilgi, deneyim ve becerileriyle beni yönlendiren, desteklerini hiçbir zaman esirgemeyen ve takıldığım her konuda yardımcı olmaya çalışan kıymetli danışman hocam Sayın Dr. Öğr. Üyesi Serpil ASLAN'a, aileme, anneme, babama ve sağlık alanındaki konularda yardımcı olan değerli eşim Fzt. Pınar GÜNDÜZ MIZRAK'a teşekkürlerimi borç bilirim.

İÇİNDEKİLER

ONUR SÖZÜ i
ÖZET ii
ABSTRACT iii
TEŞEKKÜR iv
İÇİNDEKİLER v
ŞEKİLLER DİZİNİ vii
ÇİZELGELER DİZİNİ viii
SİMGELER VE KISALTMALAR DİZİNİ ix
1. GİRİŞ 1
1.1. Tezin Önemi ve Gayesi 3
1.2. Tez Bölümleri 3
2. KAYNAK ÖZETLERİ 5
2.1. Tezin Literatüre Katkısı 5
3. MATERYAL VE METOT 7
3.1. Blok Zinciri 7
3.2. Blok Zinciri Sisteminin Temel Kriterleri 8
3.3. Blok Zinciri Teknolojisi Nasıl Çalışır 8
3.3.1. Özel (Private) blok zinciri 9
3.3.2. Açık (Public) blok zinciri 9
3.3.3. Konsorsiyum blok zinciri 10
3.4. Blok Zincirinin Uygulama Alanları 10
3.5. Blok Zinciri Teknolojisi Nasıl Çalışır 11
3.6. Genel Anahtar ve Özel Anahtar 12
3.7. Özet Fonksiyonu (Hashing) 13
3.7.1. Özet fonksiyonu algoritmaları 14
3.7.2. Özet fonksiyonun kullanım alanları 14
3.7.3 Özet fonksiyonun blok zincirdeki kullanımı alanları 14
3.8. Konsensüs 15
3.8.1. Blok zinciri uzlaşma (Konsensüs) algoritmaları 15
3.8.1.1. İş kanıtı (PoW) algoritması 16
3.8.1.2. Hisse kanıtı (PoS) algoritması 16
3.9. Veri Tabanı 16
3.9.1. Yapılandırılmış veri 16
3.9.2. Yapılandırılmamış veri 17
3.9.3. İnternetin geçmişi ve geleceği 17
3.10. Blok Zinciri ve Sağlık Sistemi 17
3.10.1. Kamu ve özel sağlık hizmetleri 17
3.10.2. Blok zinciri ve sağlık sistemi 18
3.10.3. Blok zincirsiz elektronik sağlık kayıt işlemleri 18
3.10.4. Blok zincirli elektronik sağlık kayıt işlemleri 19
3.10.5. Blok zinciri uygulaması 19
3.11. Uygulamada Kullanılan Java Teknolojileri 20
3.11.1. Spring boot 20
3.11.2. Spring data 20
3.11.3. Spring api 21
3.11.4. Spring security 21
3.11.5. Postman 21

3.11.6. Uygulama özellikleri ve modülleri 21
3.11.6.1. Super admin modülü 23
3.11.6.2. Hastane modülü 23
3.11.6.3. Doktor modülü 23
3.11.6.4. Hasta modülü 24
3.11.6.5. JWT 24
3.11.6.6. JWT çalışma mantığı 24
3.12. Blok Zinciri Uygulama Görüntüleri 26
4. ARAŞTIRMA BULGULARI VE TARTIŞMA 32
4.1. Sağlık Alanında Blok Zincir Teknolojisi 32
4.2. Tartışma 32
5. SONUÇ VE ÖNERİLER 33
6. KAYNAKLAR 35

ŞEKİLLER DİZİNİ

Şekil 3.1. Blok Zincir Görseli 7
Şekil 3.2. Blok Zincirindeki Her Bir Blok Görseli 8
Şekil 3.3. Özel (Private) Blok Zinciri Mimari Görseli..... 9
Şekil 3.4. Açık (public) Blok Zinciri Mimari Görseli..... 10
Şekil 3.5. Blok Zincirindeki Uygulama Alanlarının Görseli 10
Şekil 3.6. Kriptografi Görseli..... 12
Şekil 3.7. Genel ve Özel Anahtarların Posta Kutusu Görseli 13
Şekil 3.8. Özet Fonksiyonu Algoritma Şema Görseli..... 14
Şekil 3.9. Blok Zincirinde Özet Fonksiyonun Algoritma Kullanımı Görseli 15
Şekil 3.10. İlişkisel Veri Tabanı Örnek Görseli..... 17
Şekil 3.11. Blok Zincirsiz Sağlık Sistemi Görseli..... 18
Şekil 3.12. Blok Zincirli Sağlık Sistem Görseli..... 20
Şekil 3.13. JWT Oluşturma Görseli 25
Şekil 3.14. JWT Çalışmanın Mekanizma Görseli..... 25
Şekil 3.15. Projenin Genel Çalışması Görseli..... 26
Şekil 3.16. Proje Derleme Görseli 26
Şekil 3.17. Kayıt Olma Görseli..... 27
Şekil 3.18. Sisteme Giriş Görseli 27
Şekil 3.19. Veri Tabanına Doktor Ekleme ve Kayıt Görseli..... 28
Şekil 3.20. Veri Tabanında Doktor Kayıt Sonrası Görseli..... 28
Şekil 3.21. Veri Tabanında Doktor JWT'siz Giriş Yapma Görseli 29
Şekil 3.22. Veri Tabanında Doktor JWT'li Giriş Yapma Görseli..... 29
Şekil 3.23. Veri Tabanında Doktor Bulma Görseli..... 30
Şekil 3.24. Veri Tabanında Doktor Güncelleme Görseli 30
Şekil 3.25. Veri Tabanında Doktor Silme Görseli 31
Şekil 3.26. Veri Tabanında Hasta Silme Görseli 31

ÇİZELGELER DİZİNİ

Çizelge 4.1. Blok Zincir Uygulama Tablosu 11
Çizelge 4.2. Blok Zincirinde Güçlü ve Zayıf Yanlar Tablosu 11

SİMGELER VE KISALTMALAR DİZİNİ

API	: Application Programming Interface (Uygulama Arayüzü)
BZ	: Blok Zinciri
BTC	: Bitcoin
DATABASE	: Veri Tabanı
DBFT	: Temsil Edilen Bizans Hata Toleransı
DDLT	: Merkezi Olmayan Dağıtılmış Defter Teknolojisi
DPOS	: Temsil Edilen Bahis Kanıtı
ESK	: Elektronik Sağlık Kayıtları
ETH	: Etherium
H2DB	: H2 Veri tabanı
HASH	: Özet Fonksiyonu (Mesaj Özütü)
JWT	: Json Web Token (JavaScript Nesne Web Belirteçi)
JPA	: Java Kalıcılık Uygulama Programlama Arayüzü
JSON	: JavaScript Nesne Bildirimi
MRG	: Manyetik Rezonans Görüntüleme
MODS	: Merkezi Olmayan Dağıtık Sistemi
MD5	: Mesaj Özeti
NSA	: Ulusal Güvenlik Teşkilatı
PUBLIC	: Genel
POW	: İş Kanıtı (Proof of Work)
POS	: Hisse İspatı (Proof of Stake)
RDBMS	: İlişki Veri Tabanı Yönetim Sistemi
SHA	: Güvenli Özet Fonkisyonu Algoritması
SBFT	: Basitleştirilmiş Bizans Hata Toleransı
TDK	: Türk Dil Kurumu

1. GİRİŞ

Verilerin kâğıt formunda kaydedilmesi ve arşivlenmesi ekstra insan gücüne ihtiyaç duyulmasına sebep olduğu gibi veri giriş hatalarına da sebep olabilmektedir. Bu gibi hatalar tıbbi hatalara yol açmakta ve hasta testlerinin tekrarlanmasına da sebep olacağı için maliyetli olabilmektedir [1,2]. Hastalar tedavi süreçlerinde farklı hastaneleri ziyaret etmek zorunda kalabilmektedirler. Hastalar sağlık kayıtlarını yaşam süreleri boyunca farklı hastanelere dağıtırken önceki sağlık kayıtlarına erişmekte zorlanabilmektedirler. Aynı zamanda parçalanmış sağlık veri kayıtlarının kötü yönetilmesine de sebep olabilmektedir. Tüm bu nedenlerden dolayı tıbbi verilerin dijitalleştirilmesi, elektronik olarak depolanması gerekmektedir [3]. Hastaların tıbbı bilgilerinin saklanması ve izinsiz kişilerce ele geçmesi hastaya ve hastaneye ciddi zararlar verebilmektedir. ESK hastayla ilgili olarak bütün bilgilerinin tutulduğu ortam olmasından dolayı güvenli bir şekilde saklanması gerekmektedir. Günümüzde ki, sağlık sektörü önceki yıllara göre bilgisayar ortamında saklanmaktadır. Örneğin, manyetik rezonans görüntüleme (MRG) ve X-ışınlarından bilgisayarlı tomografiye (BT) ve ultrason taramalarından elektronik tıbbi belgeler olması bulut üzerinde taşınılabilmektedir. Burada ki bulut hizmetlerinin artan popülaritesi ile sağlık kayıtlarının bulut tabanlı platformlara taşınması sağlık ve araştırma kurumları arasında paylaşılmasını daha önce hiç olmadığı kadar kolaylaştırarak daha hızlı ve verimli bir şekilde bilgi alışverişine olanak sağlamaktadır [4]. Bulut hizmeti sağlayıcıları, depolarındaki sağlık kayıtlarını verilerin kontrolünü ve esnek paylaşımı ile yükümlüdür. Etkileşimli işbirliğini kolaylaştıran bulut tabanlı sistemlerin, tedaviler hakkında yeni bilgilerin araştırılması, analiz edilmesi ve nüfus sağlığının daha iyi yönetilmesi gibi avantajları olduğu gibi çeşitli zorlukları da beraberinde getireceği göz ardı edilmemektedir. Örneğin, yüksek boyutlu verilerin depolanması sağlık sektöründe veri yönetimi için büyük zorlukları doğurmaktadır. Sağlık kayıtlarının güvence altına alınması, uzaktan erişim ve doğrulanması sağlık sektöründe ki bir diğer büyük zorluklardan bahsedilmektedir [5]. Bu zorlukların üstesinden gelirken sağlık kayıtlarının bütünlüğünü, güvenilirliğini ve gizliliğini sağlamak esas görevlerdendir [6]. Veri sahipleri ve emanetçileri için toplanan verilerin kötü amaçlı kullanıcıların elinde savunmasız olma riski bulunmaktadır. Bu tür risklerden dolayı hizmet sağlayıcılara karşı güvensizlik ortamı oluşturmaktadır. Tüm engellerin üstesinden gelmek için

verimli depolama ve hızlı veri geri alması, güvenli veri paylaşımı ve ESK kayıtlarının güvenliğini hedef alan yeni kayıt sistemleri oluşturmaktadır [7,8].

Modern toplumlarda, tıbbi verilerin oluşturulmasında, hastalıkların tedavisi için yeni sağlık tekniklerin ortaya çıkmasında ve bu teknikleri hastalara uygulamak, iyileşmenin bir süreci niteliğindedir. Burada tıbbi verilerin dijital ortamlarda saklanmasının önemi her geçen gün artmaktadır. Büyük verilerin veri paylaşımı, veri güvenliliği, verilerin sadece ilgili kişiler tarafından kullanılmasını sağlamak ve olumsuz risklerin önüne geçmek devletlerin görevi haline gelmektedir. Bu riskleri azaltmak için ciddi yatırımlar yapılmaktadır. Bu verilerin saklanması, verilerin güvenli bir şekilde taşınmasını, verilerin klasik verilere erişimde kullanılan sisteme giriş çıkış işlemlerine yeni bir teknoloji alanı olan blok zincirinden bahsedilmektedir. Blok zinciri dağıtık bir modelleme sistemiyle oluşturulmuş, farklı teknolojilerle uyumlu ve merkezi olmayan dijital bir defter denilmektedir. Blok zincirini daha kapsamlı açmak gerekirse, güvenli veri paylaşımını sağlamak ve merkezi olmayan veri işlem bütünlüğünü korumak amacıyla tasarlanmış birçok bilgisayardaki işlemleri kaydeden ve daha sonra hiçbir şekilde geriye dönük olarak değiştirilemeyen halka açık dijital defterlerdir. Blok zinciri kelimesi bir ağda yapılan işlemlerin blok ve blokların ardı ardına zincirlenmesi ifadesinden dolayı blok zinciri adını almıştır. Yeni eklenen zincir bir önceki bloğa bağlanmakta olup, bağlanan bu zincirlerin uzun bir zincir haline gelmektedir. Sonuç olarak, blok zinciri artık kaydın adı olarak söylenmektedir. Blok zincirde veriler üzerinde işlem yapılırken her bir işlem halka açık olarak kaydedilip kontrol edildiğinden dolayı diğer yöntemlere kıyasla yüksek bir hesap verilebilirliğini sağlamaktadır. Blok zincirine girilen her bir veri için hiç kimse önceden eklenen tüm bilgileri değiştirememektedir. Diğer bir deyişle verilerin gerçek ve değişmemiş olduğunu gösteren yeni bir teknoloji adından bahsedilmektedir [9]. Blok zincirde veriler, merkezi bir veri tabanı yerine ağlarda depolanmaktadır. Bu sayede, sistemin kararlılığı artmakta ve saldırıya uğradığı anda göreceği zarar minimize edilmektedir. Blok zincirler sağlık hizmetlerinde ciddi veri gizliliği, güvenlik ve bütünlük sorunlarını çözebilecek stratejilere sahip veriler olarak söylenebilmektedir. Örneğin, sağlık sektöründe, blok zincir teknolojileri sayesinde hasta kayıtlarının gizliliği kaydedilmektedir. Blok zinciri teknolojisi, sağlık sektörü için büyük bir temel ağ ve âdemi merkeziyetçilik, değişmezlik yeteneği ve birlikte çalışabilirliğini sunmaktadır. Blok zinciri birçok teknoloji ve algoritmalarla birlikte

çalışmaktadır. Bulut teknolojisi, özet fonksiyonu algoritması örnek verilebilir. Bu teknolojilerden bulut teknolojisi sayesinde verilerin iletiminde hızlı, dinamik, veri paylaşımı sağlanır. Paylaşımların özet fonksiyonu algoritmaları kullanılarak kişilerin izni olmadan ham veri üzerinden herhangi bir değişikliğe olanak sağlamadan veri gönderimi sağlanır [10].

Bu tez kapsamında, ESK kayıtları için veri erişim kontrolü ve denetimi sağlarken bulut servis sağlayıcıları arasında sağlık verilerinin paylaşılması için JWT önerilmiştir. Önerilen bu yöntemde blok zincire yeni bir çözüm olan JWT, sistem girişi için daha güvenli ve hasta verilerinin kontrolünü sağlamak üzere merkezli bir uygulamaya geçiş hedeflenmektedir.

1.1. Tezin Önemi ve Gayesi

Bu tezde, blok zincir teknolojisinin ne olduğunu ve bu teknolojinin sağlık alanında nasıl kullanıldığını incelenmiştir. Blok zinciri erişim için klasik veri tabanı, oturum girişi yerine JWT mantığıyla sisteme giriş uygulaması örneklendirilmiştir. Blok zinciri günümüzde birçok alanda kullanılmaktadır. Bu alanlardan sağlık sektöründe, blok zinciri kullanımını nasıl olduğu incelenmiştir. Blok zincirini sağlık alanında kullanılmasıyla, veri güvenliliği ve hızlı veri paylaşımı sağlayabilmektedir. Tezin temel amacı sağlık alanında blok zincirinin nasıl kullanılacağına dair araştırmalar yapmak ve JWT ile sisteme nasıl giriş yapılacağını göstermektir. Bu araştırmalara ek olarak blok zinciri mimarisindeki önemli algoritmalar olan konsensüs algoritmaları, PoS (Proof of Stake) ve PoW (Proof of Work) algoritmasının blok zincirdeki hangi problemleri çözdüğünden de bahsedilmektedir. Tez kapsamında yapılan uygulama, yüksek seviyeli ve güvenli dil olan Java diliyle yazılmıştır. Çalışmada, spring framework tercih edilmiştir. Spring framework'un dosya yönetimi olan spring boot teknolojilerinde spring data, spring api (Application Programming Interface), spring security, JWT ve veri tabanı için H2 veri tabanı tercih edilmiştir. Bu tezde blok zincirinin sağlık alanındaki bütün sorunları çözmese de önemli problemler olan veri paylaşım hızını, veri erişimi, veri güvenliğini gibi alanlardaki sorunları üzerinde durularak çözümler önerilmiştir.

1.2. Tez Bölümleri

Tez çalışmasının üçüncü bölümü itibariyle; blok zincirinin tanımı, blok zincirinin nasıl çalıştığını, blok zincir mimarisini, blok zincirin uygulama alanlarını,

blok zincirde kullanmak üzere genel anahtar, gizli anahtardan bahsedilmiştir. Blok zincirinin güvenliğini sağlamak üzere yine üçüncü bölümde özet fonksiyonu üzerinden durulmuştur. Bahsi geçen özet fonksiyonun blok zincirdeki kullanılmasının öneminden bahsedilmiştir. Blok zincir algoritmaları olan konsensüs algoritmalarından PoS ve PoW algoritmaları incelenmiştir. Geleneksel veri tabanı, yapılandırılmış veri tabanı, internetin dünü, bugünü ve geleceği hakkında bilgiler verilmektedir. Blok zinciri sistemine giriş için JWT ile sisteme girişi sağlayıp api üzerinden Postman programıyla veri gönderip veri almada kullanılmaktadır. Postman, api (Application Programming Interface) geliştirme, test etme ve belgeleme süreçlerini kolaylaştırmak için kullanılan popüler bir yazılımdır.

2. KAYNAK ÖZETLERİ

Blok zincir tanım olarak dağıtık veri tabanı sistemi adı olarak verilmektedir. Verileri merkezi olmayan, her bir blok zincirinin bulunduğu sunucu üzerinde yaşamaktadır. Bu verilerin hasta bilgilerini bulut sistemi üzerinde taşıyarak verilerin güvenli bir şekilde iletilmesi ve bu verilerin erişilmesinde hızlılığı ve veri güvenliliği üzerinde durulmuştur. Öyle ki bu bilgilerin bulut sistemi üzerinde klasik veri saklama ve veri güvenliğini nasıl daha güvenli yapabiliriz sorusunun cevabı bu tez kapsamında araştırılmaktadır [10].

Yukarıdan bahsi geçen güvenlik durumları için ilk olarak bilgiler özet fonksiyonundan geçirilip saklanmaktadır. Her hastanın tıbbi kayıtları sadece yetkili kişiler tarafından özel olarak kullanılmaktadır. Bloğun gövdesi, işlemler için merkle ağaç kökünün özet fonksiyonu değerini içermektedir. Merkle ağacı işlemleri her yaprakta depolar ve karma değeri, doğrulama ve bütünlük verimliliğini desteklemek için yaprak olmayan düğümlerde ve her iki düğümde alt düğümlerde birleştirilerek depolanmaktadır [11].

Blok zincirinde, her bir blok ardı ardına değişmez bloklar olarak devam etmektedir. Değişmezlik, önceki bloğun özet fonksiyonu değerinin geçerli blokta depolanmasıyla uygulanan kalite özelliğidir. Her bloğun iki özet fonksiyonu değeri vardır, biri önceki bloğun özet fonksiyonu değeri, diğeri ise kendisinin özet fonksiyonu değeridir. Bu yordamda, kayıtlar üzerindeki herhangi bir manipülasyon, karma işlevinin girişini değiştirir ve sonuç olarak var olan değerden farklı yeni bir karma değeri oluşturur. Bu nedenle, açıklanan blok, sahte bir kök karması nedeniyle sistematik olarak blok zincirden arındırmaktadır [12].

Bu tez kapsamında blok zincirinde kullanılan algoritmalardan Konsensüs algoritmalarından en önemli iki algoritma olan PoW ve PoS gibi algoritmaları üzerinden durulmaktadır.

2.1. Tezin Literatüre Katkısı

Kaynak özetleri bölümünde tez kapsamında ele alınan konu başlıklarıyla ilgili literatüre değinilmiş olup, blok zincire erişim için üye girişinde JWT kullanarak sistemde daha az riskli hasta verilerinin saklanılmasından bahsedilmektedir. Sağlık alanında veri güvenliği, hızlı veri taşıma, var olan verileri bulut sisteminde saklamanın, klasik veri saklama, veri taşımaya göre blok zinciri daha uygun olduğu

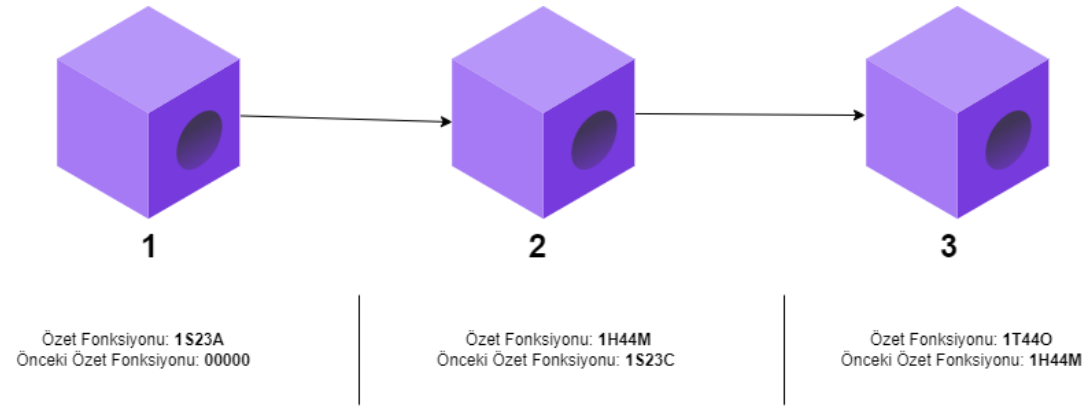
söylenilebilir. Tez kapsamında blok zinciri yeni güvenli giriş sistemi olarak JWT önerilmektedir. Sistem yapısındaki yükleri paylaştırmak için, katmanlı mimari uygulaması Java ile örneklendirilmektedir. Önerilen yöntemle blok zincirine sistem girişi daha güvenilir olması ve sistemdeki verileri bulut sisteminde taşınmasında daha kolay ve sistemi yüksek ölçeklendirilebilmesi amaçlanmaktadır.

3. MATERYAL VE METOT

3.1. Blok Zinciri

Blok zinciri, her bir verinin bloklar halinde ardı ardına eklenmesinden dolayı blok zinciri denilmektedir. Blok zincirinin görevi merkezi bir sistemi olmayan uçtan uca bağımlı kullanıcılar arasında dinamikleşerek veri paylaşımını sağlayan dağıtık mimari teknolojisidir. Blok zinciri veri güvenli, şeffaflık ilkesini benimseyerek veri paylaşımını sağlamaktadır. Blok zinciri kelimesi 2008 yılında kullanılmaya başlanmıştır. Bitcoin yani sanal para birimi kelimesi olarak 2009 kullanılmıştır [13].

Ağda doğrulanmış yöntemlerin listesi bir zincirin sonuna yeni bir metot bloğu eklenmesiyle devam ederek çalışmaktadır. Şekilde bloklar halinde veriler zincirlenerek ve şifrelenerek ardı ardına sıralanmasını gösterilmektedir. Şekil 3.1'de bir blok zinciri görselini izah edilmiştir.



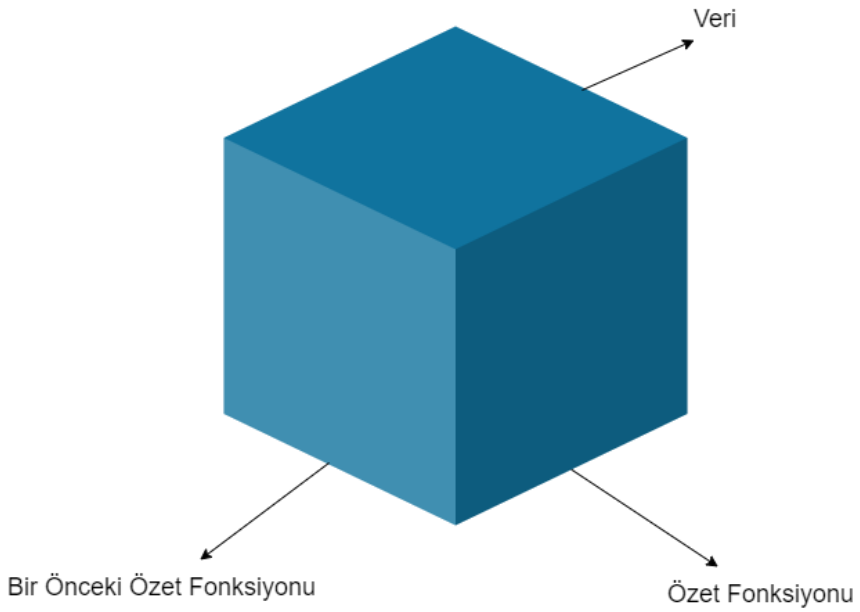
Şekil 3.1. Blok Zincir Görseli

Veri (Data): İşlenmemiş, ham bilgilere denilmektedir.

Jeton (Token): Token kelimesi İngilizce bir kelime olup Türkçe karşılığı jeton olarak bilinir. Bir platformda tüm yetkinliklerini kullanmamızı sağlayan yapının genel adı olduğu söylenmektedir.

Özet Fonksiyonu (Hash): Her bir blok ve içindeki tüm içeriklerini birbirinden tamamen farklı olması gerekmektedir. Buna örnek olarak dünyadaki her bir insanın parmak izi birbirinden farklıdır. Buradaki her bir bloğunda birbirinden farklı olması parmak izi farklılığı gibi olması gerekmektedir. Bu farklılık özet fonksiyonları kullanılarak oluşturulabilir. Oluşturulan her bir özet fonksiyonu ile bloklar arasında anahtar kilit uyumu bulunmaktadır.

Önceki Bloğun Karması (Hash Of Previous): Her blok bir önceki bloğun karmasını içermektedir. Her bloğun bir önceki bloğa göstermesi için bloklar arasında blok zinciri oluşturulması gerekmektedir. Bir blok zincirindeki, ilk blok olduğu için bir önceki bloğa işaret edemez ve buna "Genesis Block" yani ilk blok adı verilmektedir. Buradaki bloklardan herhangi birindeki değişikliğin meydana gelmesi bütün blokları etkileyeceğinden bir sonraki blok özet fonksiyonundan farklı olması beklenmektedir. Böylelikle zincirde değişme meydana geldiğinden diğer blokları etkiler ve artık eşleşmeyen bloklara dönüşmekte ve böylelikle tüm bloklar çalışamaz hale gelmektedir. Şekil 3.2'de bu durum izah edilmiştir.



Şekil 3.2. Blok Zincirindeki Her Bir Blok Görseli

3.2. Blok Zinciri Sisteminin Temel Kriterleri

Blok zincirinin temel kriterlerinden ilki dağıtık olmasıdır. Bir değeri ise şeffaflıktır. Şeffaflık; her bir verinin bir sonra ki veya bir önceki veri bloğunu doğrulayabilir olması anlamına gelmektedir. Diğer bir ilkesi değiştirilemez olmasıdır. Bloklara eklenen veriler değiştirilirse, bütün bloklar bundan etkilenir [14].

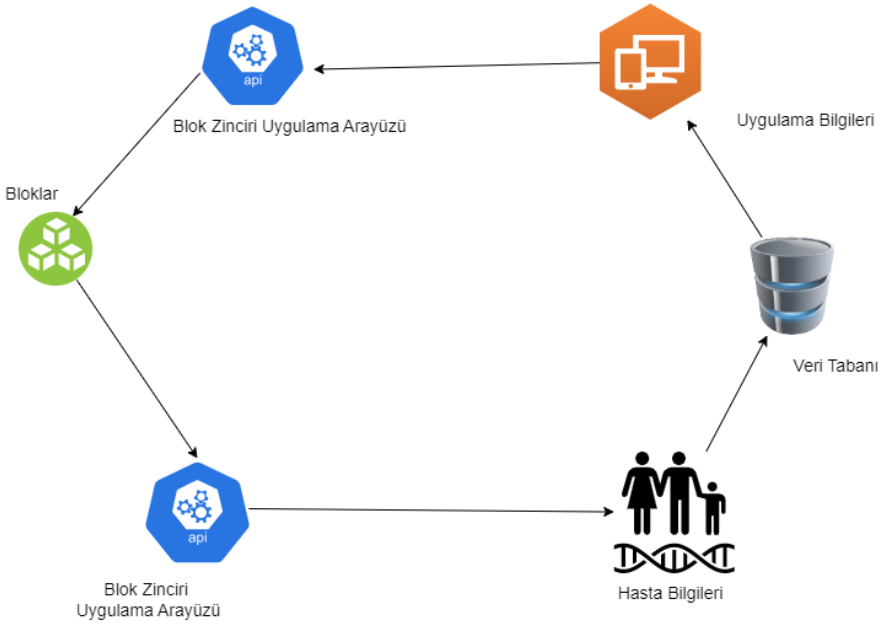
3.3. Blok Zinciri Teknolojisi Nasıl Çalışır

Blok zinciri teknolojisi üç'e ayrılır. Bunlar gizli (private) blok zinciri, açık (public) blok zinciri ve konsorsiyum blok zinciri olmak üzere üç çeşittir.

3.3.1. Özel (Private) blok zinciri

Gizli blok zinciri sistemine sahip bir ağa sadece yetkisi bulunan kullanıcılar girebilmektedir. Gizli blok zincirinde sadece izin verilen kullanıcılar sisteme giriş yapabilir. Özel blok zinciri mimarisi Şekil 3.3'te gösterilmiştir. Bu mimaride kullanıcıların basit giriş ekranında kendilerine verilen kullanıcı bilgileriyle sisteme giriş yapabilmektedir. Buradaki bilgilerin her biri api yardımıyla blok zincirine eklenmekte olup eklenen her bir blok, blok zinciri döngüsünde yer almaktadır.

Genel blok zincirinde herhangi giriş kısıtlaması bulunmamaktadır. Bundan dolayı özel blok zinciri denilmektedir. Bu zincir çeşidinde şeffaflık ve açıklık ilkesine göre çalışmaktadır [15].

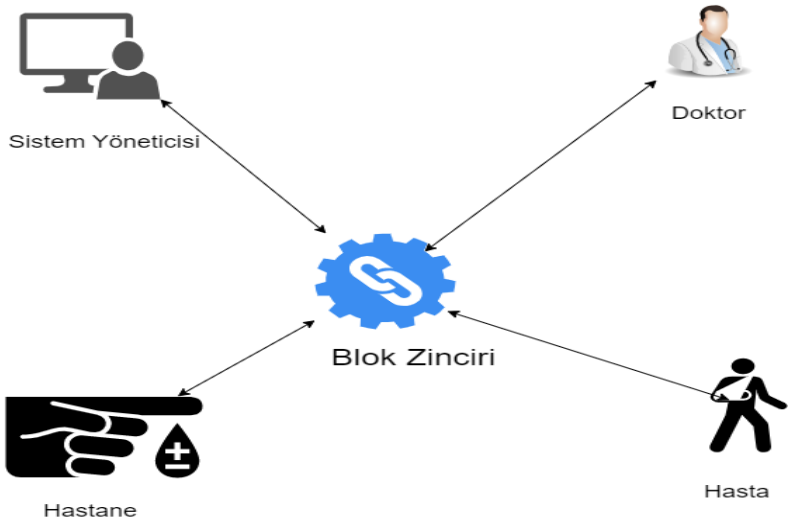


Şekil 3.3. Özel (Private) Blok Zinciri Mimari Görseli

3.3.2. Açık (Public) blok zinciri

Açık blok zinciri sistemine dileyen herkes katılabilmektedir. Merkezi bir yapıda olmayan bir sistem denilmektedir. Açık blok zinciri mimarisi Şekil 3.4'te gösterilmektedir. Açık zincir mimarisinde tüm bloklar dağıtık olarak merkezi bir noktada tutulmaktadır. Şekil 3.4'de gösterilen sistem üzerinde kullanıcı yetkisine sahip dört farklı kullanıcı kendilerine verilen rollere göre sınırlamalar getirilerek sisteme erişim sağlanabilmektedir. Kullanıcı rolleri, hasta, uzman, yönetim ve sağlık kuruluşundan oluşmaktadır. Bu rollere göre açık bir blok zinciri tasarımında

kullanıcıların kimlik bilgileri gizlenmektedir. Merkezi olmayan bu sistem, bağımsız bir blok zinciri olarak da bilinmektedir [15].



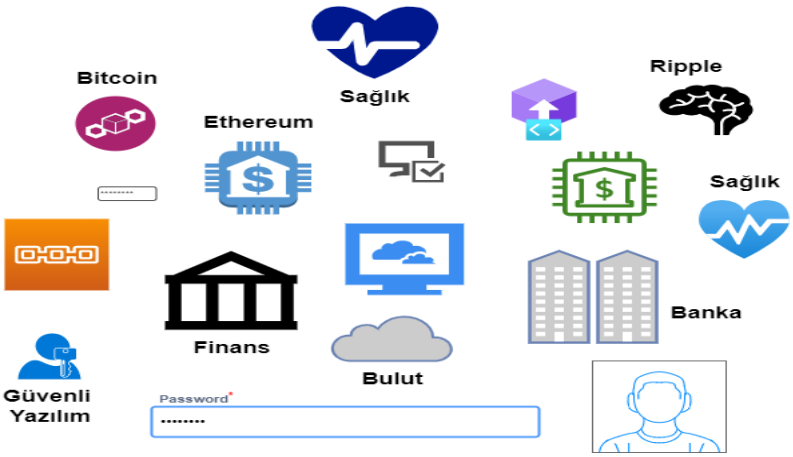
Şekil 3.4. Açık (public) Blok Zinciri Mimari Görseli

3.3.3. Konsorsiyum blok zinciri

Konsorsiyum blok zinciri, özel ve gizli blok zincirinin birleşimi denilmektedir. İsteğe göre açık veya özel blok zinciri seçimi yapıla bilinmektedir.

3.4. Blok Zincirinin Uygulama Alanları

Blok zinciri, internet dünyasında birçok alanda kullanılmaktadır. Sağlık, borsa, enerji sektöründe, sanal para alanı olan bitcoin ethereum, ödeme sistemlerinde, bulut bilişim, bahis, e-ticaret, tapu, fonlama gibi alanlarda bahsedilmektedir. Şekil 3.5'te blok zinciri uygulama alanları görseli görülmektedir.



Şekil 3.5. Blok Zincirindeki Uygulama Alanlarının Görseli

Çizelge 4.1'de blok zincirinin uygulama tablosunu ve Çizelge 4.2'de blok zincirinde güçlü ve zayıf alanların tablosu görmektedir.

Çizelge 4.1. Blok Zincir Uygulama Tablosu

Sıra No	**Uygulama Alanları**
1	Bankacılık
2	Borsa
3	Bağış Organizasyonlarında
4	Bulut Bilişim Güvenliğinde
5	FinTech
6	Para Transferi
7	Özel Bilgi Oluşturulması ve Gizlenmesi
8	E-Ticaret alanlarında ve Ödeme Sistemlerinde
9	Hisse Senetleri İşlemlerinde
10	Sağlık Alanında
11	E-Noter
12	Kamu Sektöründe
13	Enerji Sektöründe
14	E-Market
15	E-Devlet

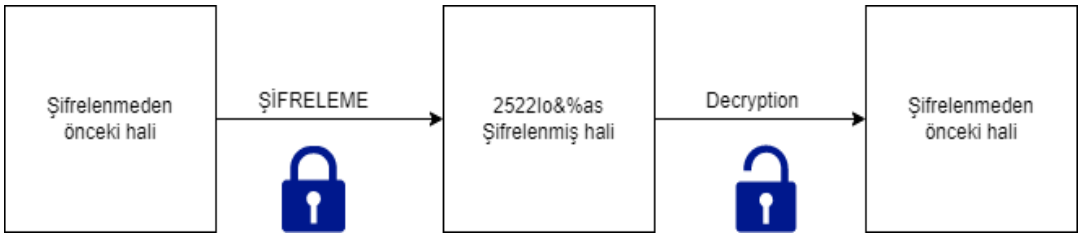
Çizelge 4.2. Blok Zincirinde Güçlü ve Zayıf Yanlar Tablosu

Sıra No	**Güçlü Yanlar**	**Zayıf Yanlar**
1	Dağıtık mimari	Yeni olması
2	Açık kaynak kodlu	Karmaşık olması
3	Şeffaflık	Veriler artıkça performans zayıflığı
4	Güvenlik	
5	Verimli olması	
6	Denetlenebilir olması	
7	Gizlilik	
8	İnsan kaynaklı hataları azaltmak	
9	Düşük maliyet	

3.5. Blok Zinciri Teknolojisi Nasıl Çalışır

Blok zinciri mimarisi farklı teknolojilerden oluşmaktadır. Bunlardan en önemlisi genel ve özel anahtarlama türü olan kriptografidir. Kriptografi *kryptós* kelimesinden türemiş Yunanca bir kelimedir. Kriptografide mesajı gönderene gönderici, mesajı alana alıcı denilmektedir. Mesajı gönderirken verilerin okunmaması durumuna ise şifrelenmiş metin denilmektedir.

Ağ üzerinden mesaj gönderildiği zaman verilere kriptografi uygulanarak şifrelenmektedir. Şifrelenmiş bu veriler sadece gönderici ve alıcıda bulunan anahtarlar yardımıyla çözülmektedir. Üçüncü bir dinleyici bu verileri dinleyememektedir. Alıcı ve verici bu verileri okuyabilmeleri içinde genel ve özel anahtarlar senkronize haberleşmesi Şekil 3.6'da kriptografi örneği görülmektedir.

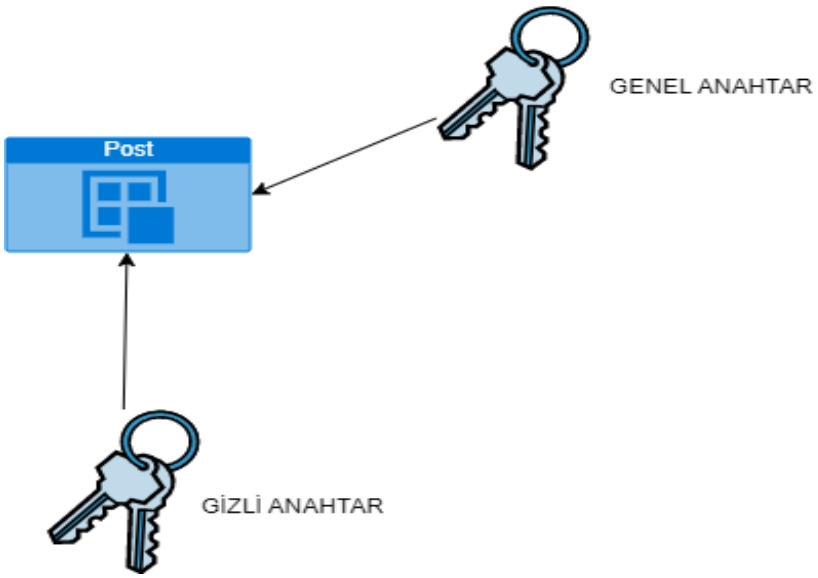


Şekil 3.6. Kriptografi Görseli

3.6. Genel Anahtar ve Özel Anahtar

Anahtarlar genel ve özel olmak üzere iki tanedir. Genel anahtar türü herkes tarafından bilinmekte olup özel anahtar türü sadece belirli bir kişide bulunmaktadır. Gizli anahtar iyi saklanmalıdır. Şekil 3.7'te genel ve özel tanımlamasını posta kutusu örneği verilmektedir. Posta kutusuna gelen postayı herkes gönderimini sağlayabilmekte ancak bunu okumak isteyen kişinin kutuyu açacak anahtarı olması gerekmektedir yoksa postaya erişim sağlanamamaktadır. Bu kutuyu açması için özel anahtarı olması gerekmektedir.

Dijital imza, blok zinciri verilerinin güvenliğini ve bütünlüğünü sağlamada kullanılmaktadır. Dijital imzalarda, simetrik olmayan yani asimetrik kriptografi görülmektedir. Blok zincirini kullanan her kullanıcıda, gizli ve açık olmak üzere iki tane anahtar bulunmaktadır. Gizli anahtar, imzalama yapmak için kullanılır. İmzalanan her bir anahtar blok zincirinde açık bir anahtar olarak yayımlanmaktadır [15].

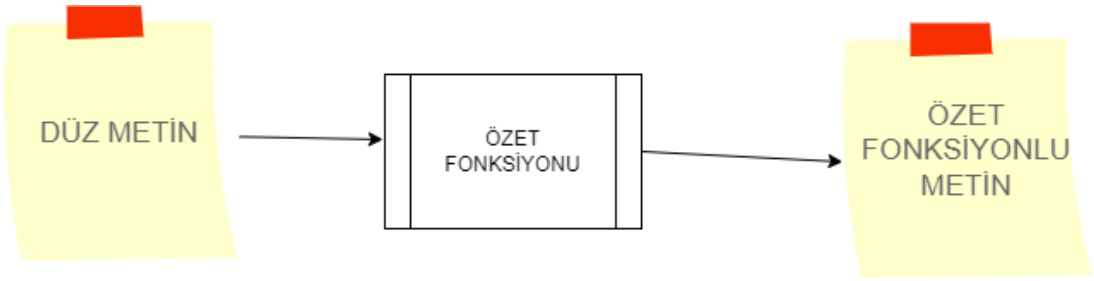


Şekil 3.7. Genel ve Özel Anahtarların Posta Kutusu Görseli

3.7. Özet Fonksiyonu (Hashing)

Özet fonksiyonu, verilerin çıktıları her zaman sabit, benzersiz ve veri bütünlüğünde kullanılmak üzere oluşturulmuş matematiksel fonksiyonlardır. Özet fonksiyonlarında her zaman aynı değer için her zaman aynı çıktı elde edilmektedir. Farklı veriler için ise her zaman farklı değer kümesini oluşturmaktadır.

Hash'in Türkçe karşılığı mesaj özütü anlamına gelmektedir. Kısaca özet fonksiyonunun farklı boyuttaki veriler için sabit boyutta çıktı oluşturmak istediğimizde kullanılmaktadır. Özet fonksiyonu algoritması, bir takım matematiksel süreçlere maruz bırakılarak sabit boyutlu veriler oluşturulmaktadır. Şekil 3.8'de bu durum izah edilmiştir. Özet fonksiyonu kriptografi alanında sıkça kullanılmaktadır. Özet fonksiyonu sayesinde blok zinciri, dağıtık sistemlerde veri bütünlüğünü, veri güvenliliği sağlamakla görevlidir. Özet fonksiyonlarının tek yönlü algoritmalardır. Tek yönlü olması ilk girdiye erişmek mümkün değildir. Şifreleme algoritmaları ise çift yönlü olarak kullanılmaktadır. Özet fonksiyonu deterministtik olup bütün girdilerde aynı sonucu elde edilir. Özet fonksiyonu kaba kuvvet saldırılarına karşı dayanıklıdır. Şekil 3.8'de özet fonksiyonu algoritma şeması görülmektedir.



Şekil 3.8. Özet Fonksiyonu Algoritma Şema Görseli

3.7.1. Özet fonksiyonu algoritmaları

Özet fonksiyonu algoritmaları, farklı büyüklükte bitlerde olup ancak ve ancak her bir algoritmada her zaman aynı girdide her zaman aynı çıktı vermesi durumudur.

Özet fonksiyonu algoritmaları arasında MD5, SHA, RIPED-D çeşitleri bulunmakta ve MD5 algoritması güvensizliği nedeniyle SHA çok daha kullanılmaktadır. MD5 128 bit uzunluğunda, MD6 256 bit uzunluğundandır. SHA Türkçesi güvenli özet fonksiyonu algoritması anlamına gelmektedir.

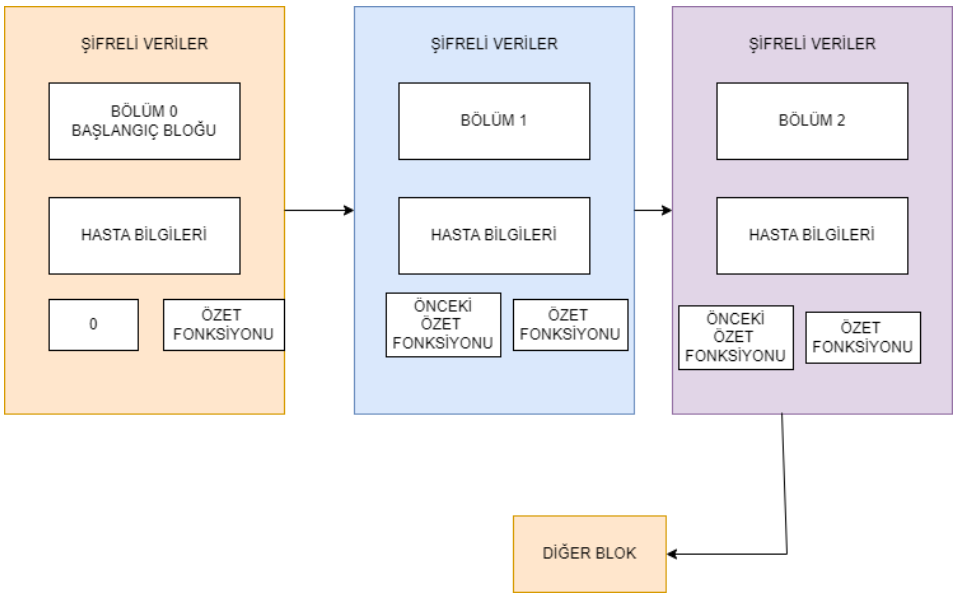
3.7.2. Özet fonksiyonun kullanım alanları

- Şifre koruması
- Kimlik doğrulama
- Dijital parmak izi
- Veri güvenliğinde
- Bilgi güvenliği
- Rootkit tespiti
- Sitelere güvenli giriş için gibi alanlarda kullanılmaktadır.
- Socket programlama (Mesaj Doğrulama)
- DNA dizilerindeki benzer dizilimleri arayıp bulmada

3.7.3 Özet fonksiyonun blok zincirdeki kullanımı alanları

Blok zincirinde özet fonksiyonlarından SHA-256 algoritması kullanılmaktadır. Özet fonksiyonu farklı büyüklükteki verilerden sabit büyüklükte çıktı almayı sağlamaktadır. Blok zincirde veri güvenliğini sağlamak ve her zaman aynı çıktıyı almak için kullanılmaktadır. Özet fonksiyonu matematiksel formüller

yardımıyla veri bütünlüğü ve güvenirliği sağlanmaktadır. Şekil 3.9'da blok zincirinde özet fonksiyonu algoritma kullanımının görseli görülmektedir.



Şekil 3.9. Blok Zincirinde Özet Fonksiyonun Algoritma Kullanımı Görseli

3.8. Konsensüs

Konsensüs Fransızca kökenli bir kelime olup, TDK'a göre "uzlaşma yada uzlaşım" anlamına gelmektedir. Konsensus algoritmaları, sistemde var olan gruptakilerin geri kalanlar arasında en iyisi olduğuna karar verip ve iyi olanı bulup seçen algoritmadır. Bir konsensüs algoritması, konsensüs kurallarının ortak bir alanda çalışmaya zorlayarak blok zincirinde kontrolü merkezsizleştirmektedir [16].

3.8.1. Blok zinciri uzlaşma (Konsensüs) algoritmaları

Uzlaşma algoritması dağıtık sistemlerde verilerin güvenlik düzenlemesiyle görevlidir. Ağ güvenliğinin sağlanması ve birbiriyle etkili iletişim kurmayı amaçlamaktadır. Blok zincirinde eşitlik ve sistemde düzenliliği sağlamaktadır. Konsensüs algoritmasında eğer en küçük bir anlaşmazlık durumda sistem kendi içinde anlaşmazlığa giderse, algoritma bu durumda topluca karar vererek uygun düğüme oy vererek yeni düğüm seçmektedir.

Merkezi olmayan dağıtık sistemlerde bu algoritmalar kullanılmaktadır. Konsensus algoritmaları on üçten fazla algoritması bulunmaktadır. Ancak bunlar arasında en önemli algoritmalar: PoW ve PoS algoritmasıdır.

3.8.1.1. İş kanıtı (PoW) algoritması

İş kanıtı algoritması blok zincirinin ilk algoritma olmasından dolayı önemlidir. Bitcoin, Ethereum, PoW algoritmasını kullanmaktadır. Blok zincirinde, bir emir verildiğinde algoritma problemlerini çözmeye başlar, zincirin güvenliği sağlamak kullanılır. Blok zincirinde yapılan bir emrin blok zincirine eklenmesinde özet fonksiyonu üretmesi için Proof of Work algoritması kullanılır. Proof Of work bitcoin için sha-256, litecoin scrypt, ethereum ise equihash kullanmaktadır [16].

3.8.1.2. Hisse kanıtı (PoS) algoritması

Hisse kanıtı kelimesini ilk defa quantum Mechanic isimli bir kişi tarafından 2011 yıllarında söylenmiş bir kelimedir. Karmaşık çözümler yerine var olanla yetinmeye çalışmaktadır. PoW algoritmasında her bir bloğun doğrulu doğrulayıcılar tarafından yapılmaktadır. Ağ içinde coin değeri en büyük olan düğüm seçilir. Eğer bu en büyük düğüm onaylanmaz veya gecikirse bundan sonraki en büyük düğüm seçilmektedir [16].

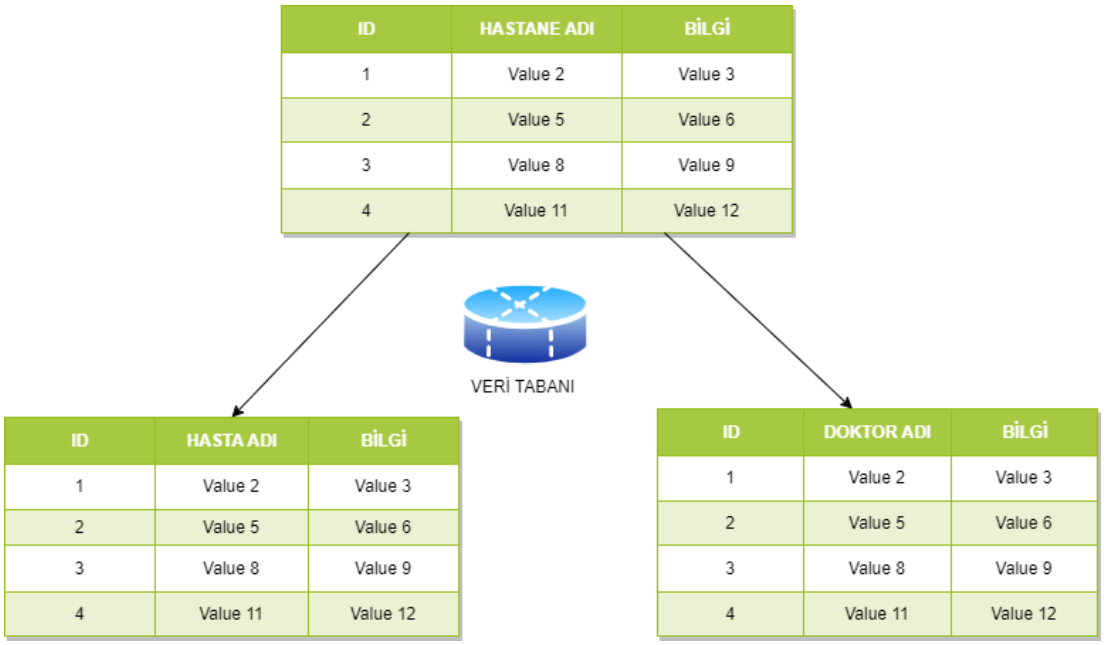
3.9. Veri Tabanı

Veri: İşlenmemiş bilgi denilmektedir. Veri tabanı, blok zinciri için önemli bir teknolojisi olup geleneksel olarak veriler yapılandırılmış veri ve yapılandırılmamış veri olmak üzere ikiye ayrılmaktadır.

Veri tabanı: 1960'ların başında ortaya atılmış bir terimdir. Veri tabanı bilgileri düzenli saklamak, yönetilmek, verileri tekrarsız olarak saklamak, her bir veriye ulaşmak kolay olmasını sağlamak ve birbirleriyle ilişkili bir biçimde düzenli olarak kaydetmeye denilmektedir.

3.9.1. Yapılandırılmış veri

Satır ve sütunlardan oluşan, her bir tabloda benzersiz bir id olması gereken veri türüdür. Şekil 3.10'de ilişkisel veri tabanı tablosunu göstermektedir.



Şekil 3.10. İlişkisel Veri Tabanı Örnek Görseli

3.9.2. Yapılandırılmamış veri

Günümüzdeki birçok veri türüne denilmektedir. Örneğin: E-posta verileri, sosyal medya verileri yapılandırılmamış veri örneğidir.

3.9.3. İnternetin geçmişi ve geleceği

İnternet hayatımıza 1969 senesinden bu zamana kadar gelmiş içerisinde veri iletiminden sorumlu teknoloji bulunan bir yapıdır. Arpanetin kurulmasından sonra daha büyük bir ivme kazanarak ilk internet çalışmalarının hızla geliştiği görülmektedir. İnternetin gelişimi her geçen gün katlanarak ivme kazanmaktadır. Gelişen teknolojilerden, yapay zekâ, makine öğrenimi, bulut teknolojileri gibi teknolojilerle her geçen gün büyümektedir.

3.10. Blok Zinciri ve Sağlık Sistemi

Sağlık günümüzde insan yaşamı için çok önemli bir role sahip olup insan hayatında önemli bir etkendir. Blok zinciri teknolojisi, sağlık verilerin taşınmasında, veri güvenliliğinde şüphesiz önemli olarak görülmektedir [6].

3.10.1. Kamu ve özel sağlık hizmetleri

Sağlık sistemi kamu sağlık sistemi ve özel sağlık sistemi olarak iki kısımda ayrılmaktadır. Kamu sağlık hizmetleri var olan hükümet tarafından karşılanıp, özel sağlık sistemi ise bireylerin sağlık sistemlerini kendileri karşılamaktadır.

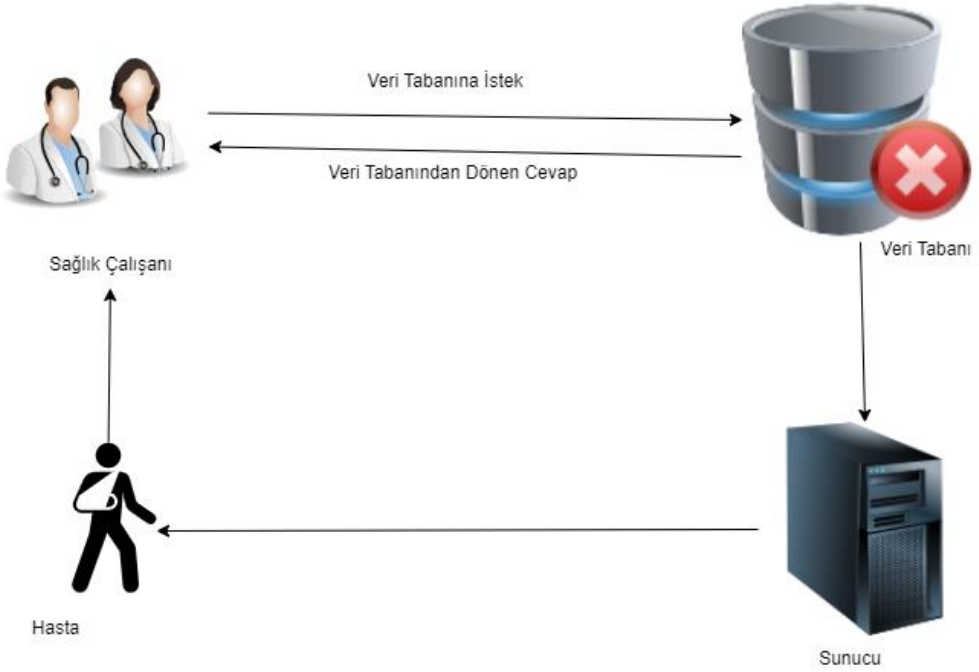
3.10.2. Blok zinciri ve sağlık sistemi

Teknolojinin ilerlemesiyle beraber sağlık alanında da ilerlemeler kaydedilmiştir. Sağlık hizmetlerinde veri güvenliği, veri paylaşımı, veri transferi için teknolojilerden yararlanılmaktadır.

3.10.3. Blok zincirsiz elektronik sağlık kayıt işlemleri

Verilerin taşınmasında bulut ortamı kullanılması, veri transfer kolaylığı sağlasa da, beraberinde veri güvenlik sorununu da ortaya çıkarılmaktadır. Veri paylaşımında, hastanın kişisel bilgileri yanlış kişiler tarafında ele geçirilmesine neden olabilmektedir. Bu durum hastanın özel bilgileri diğer kişiler tarafından ele geçirebilir ve kötü sonuçlar doğurabilmektedir. Bu risklerden kaçınmak veri erişiminin yetkilendirilmesi, verileri şifreleyerek gönderilmesi, veri tabanının muhafaza edilmesi ve saklanması son derece hayati öneme sahip olmaktadır [6].

Şekil 3.11'de elektronik sistem üzerinden yetkili kişilerce verilere erişmesi ve yetkilendirilmiş durumunu görmektedir. Blok zinciri olmadan yapılan sistem bilgilerine erişmek aslında çok güvenli olduğu söylenmemektedir.



Şekil 3.11. Blok Zincirsiz Sağlık Sistemi Görseli

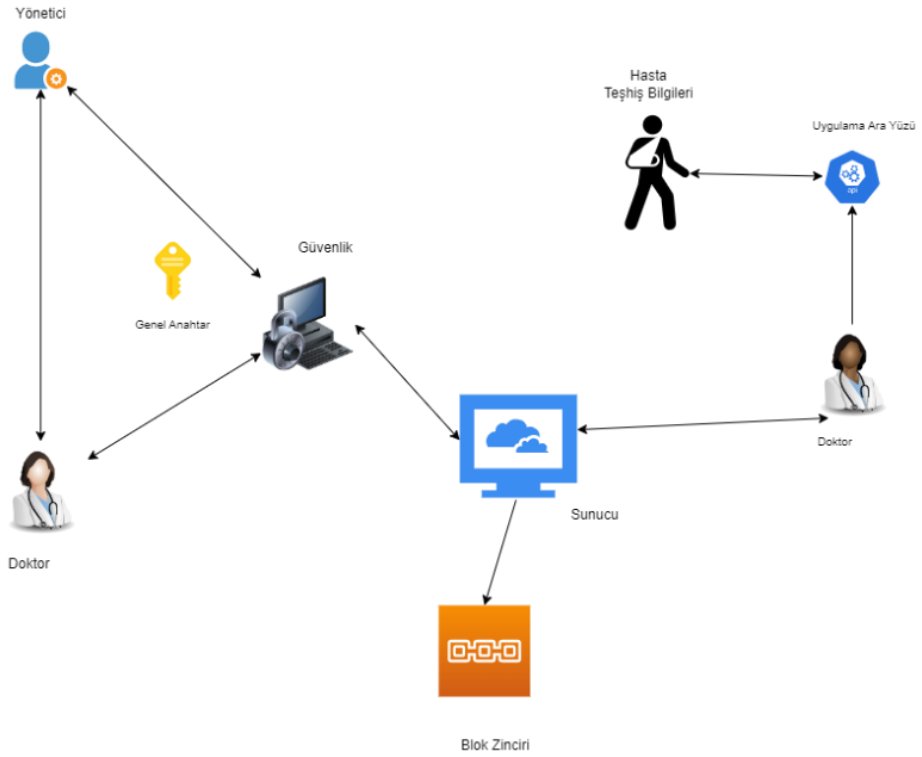
3.10.4. Blok zincirli elektronik sağlık kayıt işlemleri

Blok zinciri sisteminde veriler şifrelenmiş olarak veri iletimi sağlanmaktadır. Verilerin girişi için rol ve imza ile veri tabanına kaydedilmektedir. Verilerin blok zinciriyle gönderilmesi, kaydedilmesi işlemlerinde gizlilik, güvenlik ve veri bütünlüğü sağlayabilmektedir.

3.10.5. Blok zinciri uygulaması

Blok zinciri uygulamasında Java Spring Boot kullanılmaktadır. Spring Boot teknolojilerinden spring data, spring security, spring rest, spring api teknolojileri kullanılmaktadır. Blok zinciri otomasyon sistemine giriş yapılmadan öncesinde bir takım sisteme kayıt ve giriş işlemlerini yerine getirmektedir. Doktor veya hasta sisteme giriş yapabilmesi için öncelikle sisteme kayıt olmaları gerekmektedir. Sisteme kayıt olduktan sonra hastane veya sistem kurucusu tarafından onay verildikten sonra sisteme giriş yapabilmektedir. Hastane veya sistem kurucusu sisteme giriş yapmış bir doktor hasta bilgilerini sisteme ekleyebilmektedir.

Blok zincirine veriler gönderildikten sonra değişim söz konusu değildir. Bundan dolayı veriler son halini aldıktan sonra blok zincirine eklenmektedir. Hasta bilgileri bloklar halinde özet fonksiyonunu dâhilinde blok zincirine eklenmektedir. Her bir hasta için ayrı bir blok zinciri vardır. Eğer bu hasta bilgilerinden bir tanesi bile değişirse blok zincirinin kırılmaktadır. Hasta sisteme giriş yaptıktan sonra bilgileri şifrelenmiş bir şekilde saklanmakta ve kendisiyle alakalı teşhis bilgilerini görebilmekte ancak bilgileri değiştirememektedir. Blok zinciri sağlık sistem görseli Şekil 3.12’de gösterilmektedir. Admin günlük olarak eklenen hasta bilgilerini görmekte ve hasta bilgilerini değiştirildiğinde veri tabanı üzerinde veya log dosyasında takip edebilmektedir. Doktor hastasının teşhis bilgilerini ekledikten sonra blok zincirine gönderebilmektedir.



Şekil 3.12. Blok Zincirli Sağlık Sistem Görseli

3.11. Uygulamada Kullanılan Java Teknolojileri

Uygulamada kullanılan Java teknolojilerinin isimleri aşağıda gösterilmiştir.

3.11.1. Spring boot

Spring Framework ile geliştirilen kurumsal projelerde kullanılan otomatik konfigürasyonları sağlayan Spring tabanlı uygulama geliştirme platformunun genel adı olarak söylenmektedir. Modüler yapıya sahip bileşenleri bulunmaktadır. Projede kullanılan modülleri, spring data, spring api, spring security modülleri kullanılmaktadır. Üçüncü parti uygulamalarından; lombok, model mapper, gson, swagger, validation, actuator kullanılmaktadır.

3.11.2. Spring data

Hasta bilgilerini, doktor bilgilerini, hastane verilerini saklamak ve gerektiğinde bu verilere erişim sağlamak istenildiğinde kullanabilecek teknoloji alanlarındandır. spring data, hibernate veya JPA (Java Persistence API) Java sınıf yapısına göre ekleme yapıldığında yönetilmesi ve eklemesi geleneksel veri tabanı yapısına göre daha kullanışlı bir yapıda olduğu söylenilebilir.

İlişkisel veri tabanı için application.properties üzerinde gömülü veri tabanı olan H2 veri tabanı kullanılarak, H2 veri tabanına erişim sağlayabilmek için ise “http://localhost:8080/h2-console” üzerinden kullanıcı adı ve şifresi verildikten sonra veri tabanında erişim sağlanır.

3.11.3. Spring api

Spring api farklı cihaz haberleşmesinde kullanılmak üzere api yardımıyla daha geniş bir proje etkinliğini sağlayabilmektedir. Api document yapısı için swagger kütüphanesi kullanılmaktadır. Bu teknoloji sayesinde api, listelemek, silmek, bulma işlemleri rahatlıkla yapılabilir. Bu api isteklerini, “http://localhost:8080/swagger-ui.html” linki üzerinden gerçekleştirmektedir.

Lombok: Java sınıflarında daha az kod ve okunabilirliği artırmak önerilmektedir. Lombok için Annotationlarda @Data, @AllArgConstructor, @NoArgsContructor v.b annotation kullanılmaktadır.

3.11.4. Spring security

Sisteme giriş güvenliliği oluşturmak için kullanılan Java teknolojisinin adına denilmektedir.

3.11.5. Postman

Postman yukarıdaki tanımda da bahsedildiği gibi Spring api ile yazdığımız api’leri test edebilmemiz için gerekli istek uygulamasının adına denilmektedir.

3.11.6. Uygulama özellikleri ve modülleri

- Sisteme giriş işlemlerinde oturum yerine JWT http üzerinden girişler daha güvenli olmaktadır. Bundan dolayı veri tabanı sisteme giriş yaptıktan sonra bilgiler veri tabanından sorgu yerine JWT üzerinden oturum olmadan sisteme girişi tercih edilmektedir.
- Hasta bilgilerini şifreleyerek (maskelemek) veri tabanından saklanmaktadır.
- Veri tabanı sisteme entegre edilerek saklanan bu veri tabanı erişim sağlamak için application.propertis'te verilen ayarlama dosya adı verilen bu yapıyı kullanarak sisteme giriş yapılmaktadır.
- Sistem katmanlı mimari yapısına göre yazılımı kodlanmaktadır.

- Yüksek seviyeli bir dil olan Java dili üzerinde kodlanmış olup Java’nın son teknolojisi olan Spring Boot kullanılmaktadır.
- Kütüphane bağımlılığını ortadan kaldırmak için Maven iskeleti kullanılmaktadır.
- Sistemde meydana gelebilecek bütün hataları log dosyasında saklanmaktadır.
- Java sınıflarında daha az kod yazmamızı sağlamak için Lombok Kütüphanesi tercih edilmektedir.
- Api document için Swagger Kütüphanesi kullanılmaktadır
- Entity ile dto sınıfları arasında değişim için model Mapper Kütüphanesi tercih edilmektedir.
- Giriş işlemlerinde oturum yerine JWT http üzerinden girişler daha güvenlidir. Bundan dolayı klasik veri tabanı sisteminden sorguya göre giriş yerine JWT üzerinden oturum olmadan sisteme girişi sağlanmaktadır.
- Hasta bilgilerini gizleyerek veri tabanda saklanmaktadır.
- Veri tabanı sisteme entegre edilerek saklanmaktadır. Bu veri tabanı erişim sağlamak için application.propertis'te verilen bilgilere göre sisteme giriş yapılmaktadır.
- Sistem katmanlı mimari yapısına göre işlenmektedir.
- Yüksek seviyeli bir dil olan Java kullanılmış olup ve Java’nın son teknolojisi olan Spring Boot kullanılmıştır. Spring Boot teknolojisinde, Spring Data, Spring Rest, Spring Security kullanılmaktadır.
- Kütüphane bağımlılığını ortadan kaldırmak için Maven iskeleti tercih edilmektedir.
- Sistemde meydana gelebilecek bütün hataları log dosyasında saklanmaktadır. Böylelikle sistem izlenmesi yapılmaktadır.
- Java sınıflarında daha az kod yazmamızı sağlamak için lombok kütüphanesi kullanılmaktadır.

- Entity ile dto sınıfları arasında değişim için ise model mapper Kütüphanesi uygulamada kullanılmaktadır.

3.11.6.1. Super admin modülü

Bu modülde güvenli giriş sistemi olan JWT ile sisteme giriş yapılmaktadır. Admin ile bütün modüllere erişim sağlanmaktadır. Hastanede çalışan doktorların bilgilerinin güncellenmesi, sistem bakım işlemlerinde sorumlu ve sistemde meydana gelebilecek sorunları izlemek ve çözümlemekle sorumlu modüldür. Sisteme izinsiz giriş yapmaya çalışan kişilerin listesi loglama yöntemiyle görebilmektedir. Doktor, hasta ve hastanenin sisteme giriş yaparken yanlış bilgiyle giriş haklarından doğan kullananım askıya alınmışsa aktifleştirmekle de sorumludur. Sisteme yapılan kaba kuvvet saldırılarında sunucuyu güvence altına alan modüldür. Veri tabanı verilerine erişim sağlayabilmesi için application.properties'e eklediği kullanıcı adı ve şifresi ile erişim sağlayabilmektedir. Sistemden backup almakla sorumludur. Sistemin olası saldırılarına karşın sunucuyu kapatma yetkisi bulunmaktadır.

3.11.6.2. Hastane modülü

Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve kullanıcı şifresi ile sisteme JWT aracılığla sisteme giriş yapılmaktadır. Hastanede çalışan sağlık personeli sisteme eklenmesini, hasta bilgilerinin yönetildiği modüldür. Doktor veya hastanın kendisine tanınan giriş haklarında yanlış girdiklerinde aktifleştirmede sorumludur. Doktor ve hastanın bilgilerine erişim sağlayabilmekte ve çıktısını alabilmektedir. Hastanesinde ayrılacak sağlık çalışanın bilgisini sisteme eklemekte sorumludur. Sağlık çalışanların sisteme eklediği bilgileri teşhisi görebilmektedir.

3.11.6.3. Doktor modülü

Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve şifresi ile sisteme JWT aracılığıyla giriş yapmaktadır. Hasta bilgilerini, teşhisini sisteme kayıt etmekle sorumlu modüldür. Hastanedeki hasta bilgisine erişim sağlayabilmektedir. Blok zincirine göndermeden önce değişiklikler yapabilmektedir. Blok zincirine kayıt edildiğinde herhangi bir değişiklik yapamamaktadır. Doktorlar hastaların bilgilerine hızlı ve güvenli erişimi hasta teşhisinde önemli bir rol oynamaktadır.

3.11.6.4. Hasta modülü

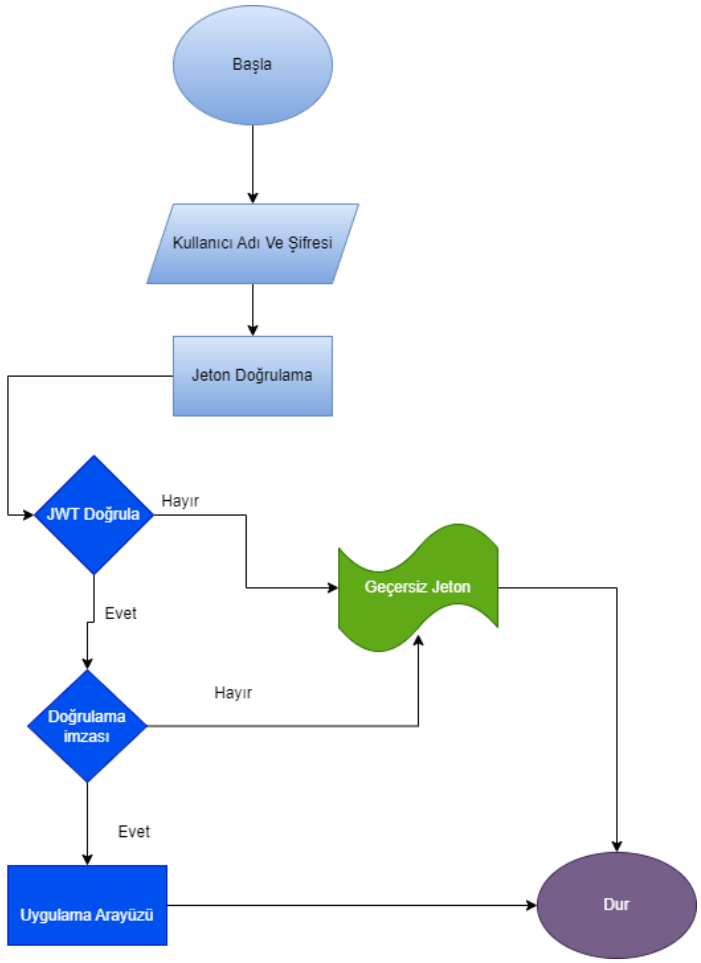
Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve kullanıcı şifresi ile sisteme JWT aracılığıyla sisteme giriş yapmaktadır. Bu modülde doktor tarafından sorulan bilgileri cevaplayacak modüldür. Hasta kendi bilgilerini okuyabileceğini ancak değiştirememektedir.

3.11.6.5. JWT

JWT Json Web Token kısaltılmasıdır. RFC7519 endüstri standardına göre hazırlanmıştır. Uygulamalarda yetkilendirme ve kimliklendirme yapmak amacıyla kullanılmaktadır.

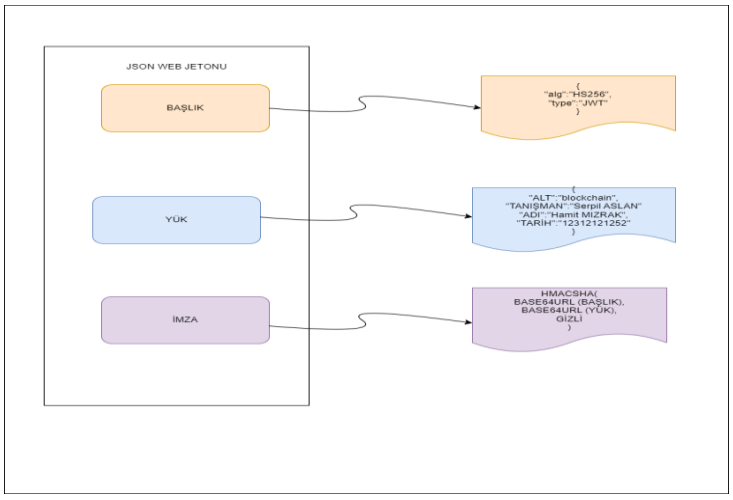
3.11.6.6. JWT çalışma mantığı

İstemci, istemde bulunur. Sunucu bu gelen isteği kontrol eder eğer tanıdığı bir token döndürüyorsa sisteme girişi sağlanır ve http Status olarak 200 döner. Eğer sistemde böyle bir bilgi yoksa yetkisiz giriş uyarısı olan UnAuthorized ve http status olarak 401 dönmektedir. Şekil 3.13, JWT oluşturma sürecini göstermektedir. Bu şemada eğer sistemde kullanıcı yoksa sisteme üye olması gerektiği, eğer üye olunmuşsa kullanıcı sistem tarafında verilen jeton ile sisteme giriş yapmaktadır. Eğer kullanıcının jeton süresi dolmuşsa sistem tarafından tekrardan jeton (token) üretmelidir. Böylelikle kullanıcı sisteme giriş yapabilmektedir.



Şekil 3.13. JWT Oluşturma Görseli

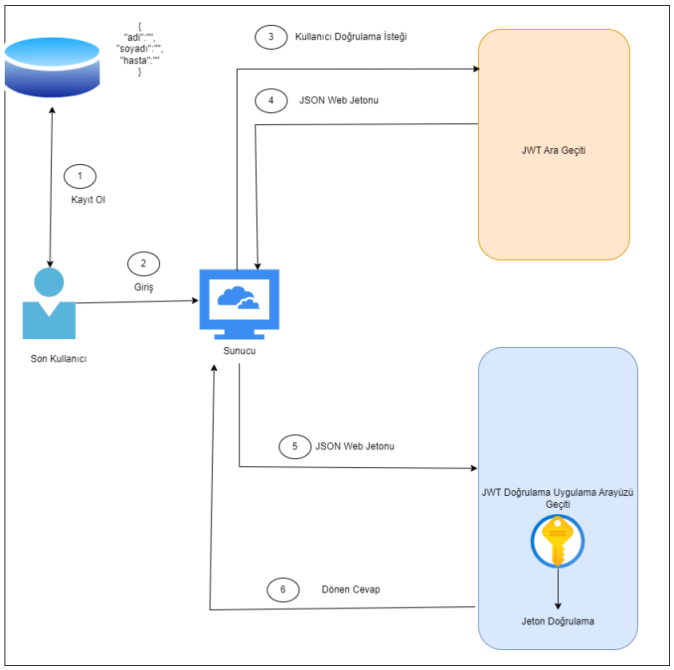
Şekil 3.14, JWT çalışma mekanizmasını göstermektedir. JWT üretilen token yapısı base64 formatında kodlanır ve 3 kısımdan oluşur. Başlık, veri, imza kısımlarından oluşmaktadır. Başlık json biçiminde oluşturulmaktadır.



Şekil 3.14. JWT Çalışmanın Mekanizma Görseli

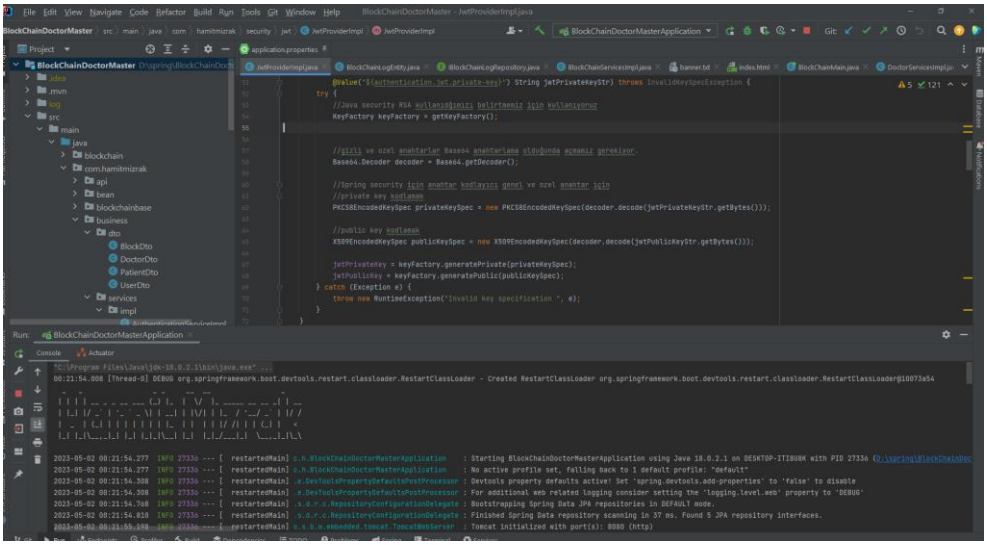
3.12. Blok Zinciri Uygulama Görüntüleri

Şekil 3.15'te proje çalışması şemasını gösterilmektedir. Uygulamaya giriş yapılması için önceden kayıtlı olunması gerekir. Kayıtlıysa sisteme giriş yapılmaktadır.

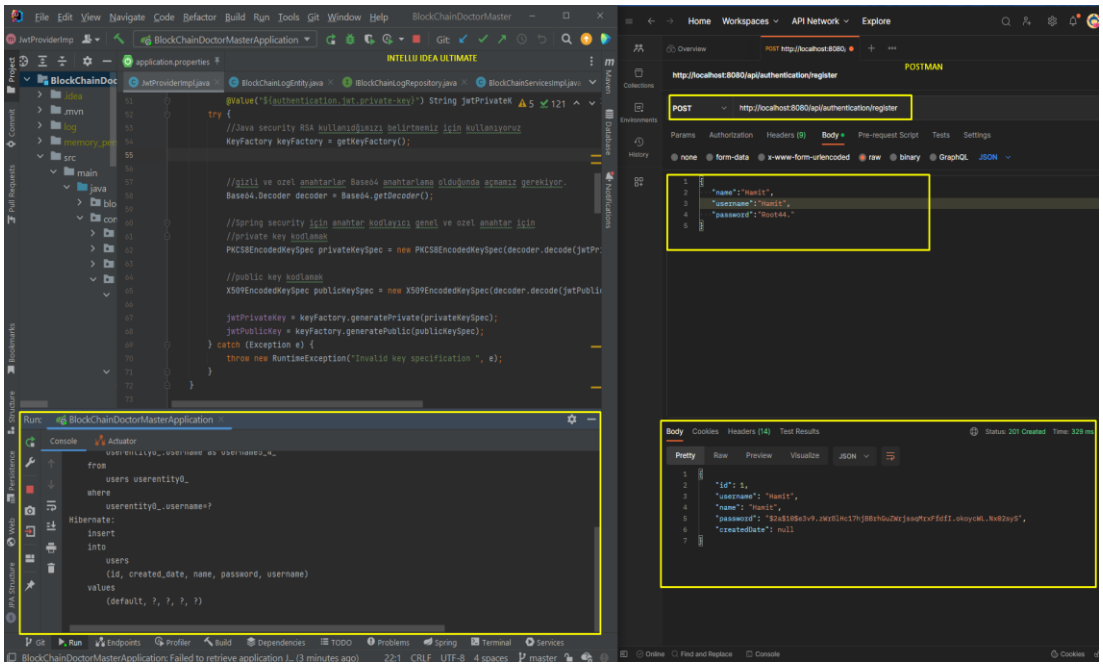


Şekil 3.15. Projenin Genel Çalışması Görseli

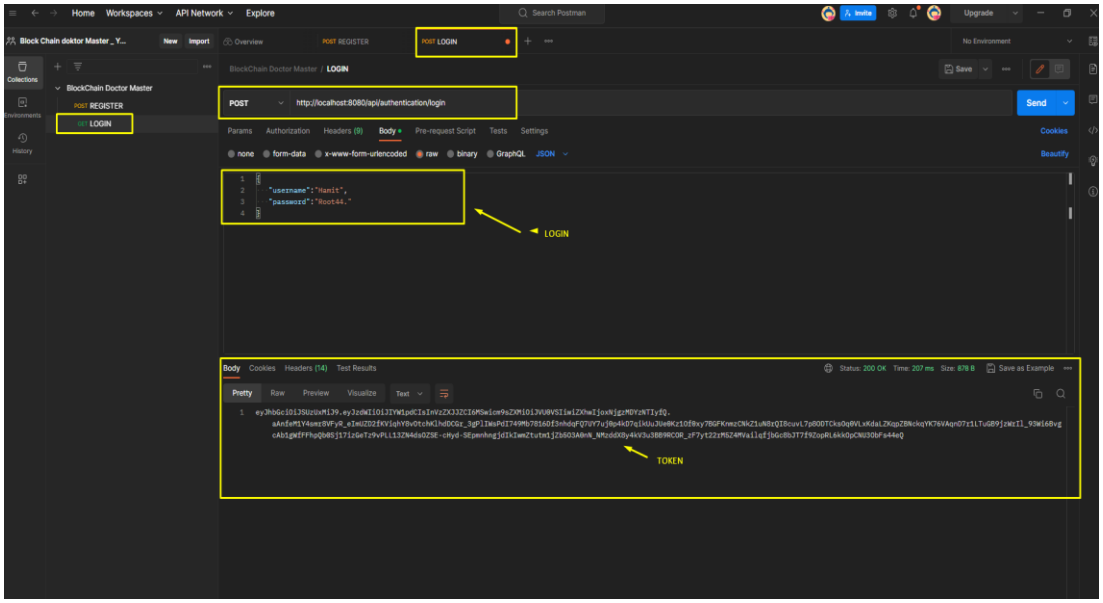
Şekil 3.16'da blok zincirinin Java Spring Boot projesinin ekran görüntüleri gösterilmektedir.



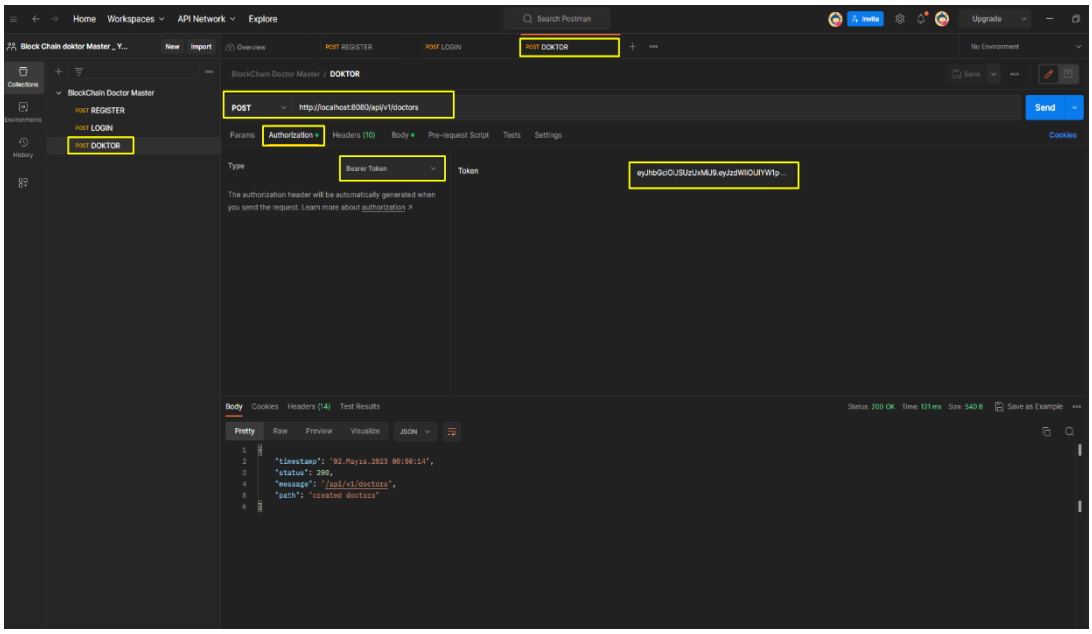
Şekil 3.16. Proje Derleme Görseli



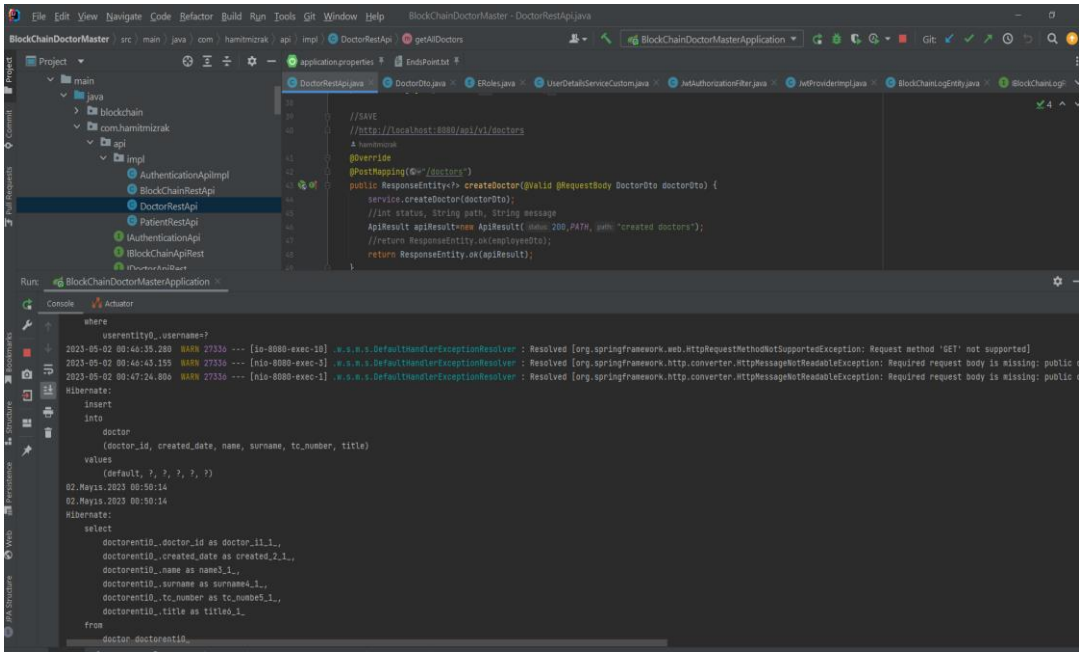
Şekil 3.17. Kayıt Olma Görseli



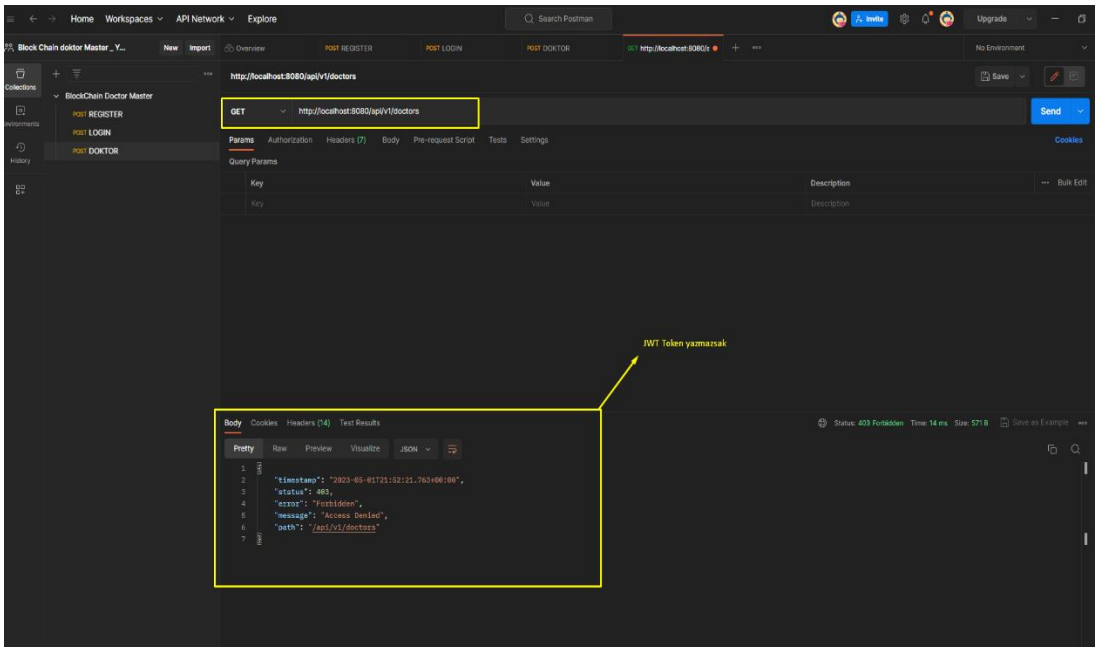
Şekil 3.18. Sisteme Giriş Görseli



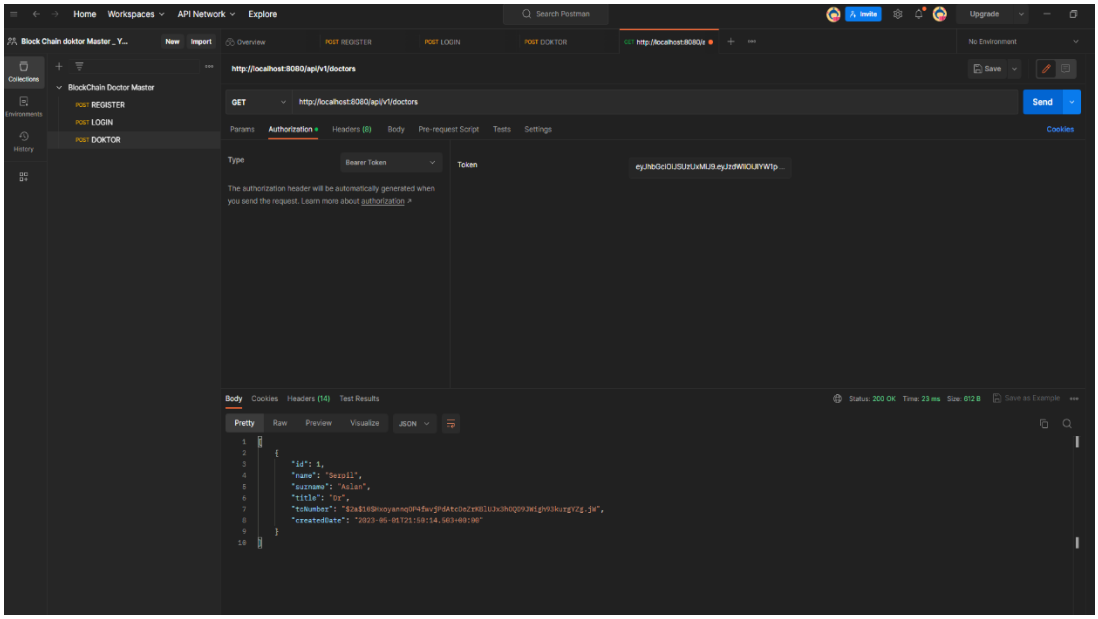
Şekil 3.19. Veri Tabanına Doktor Ekleme ve Kayıt Görseli



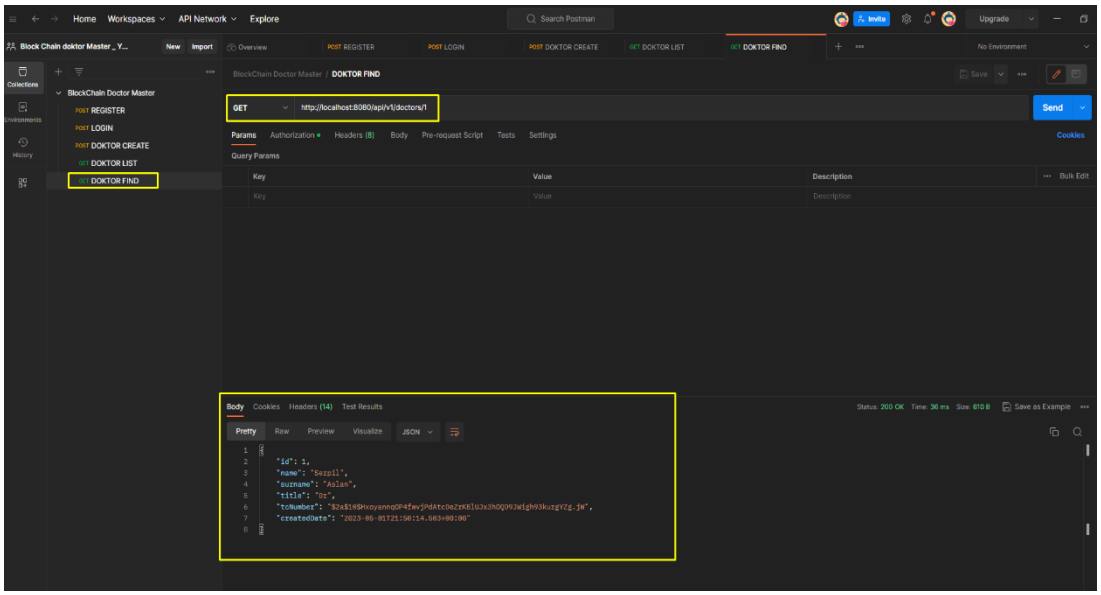
Şekil 3.20. Veri Tabanında Doktor Kayıt Sonrası Görseli



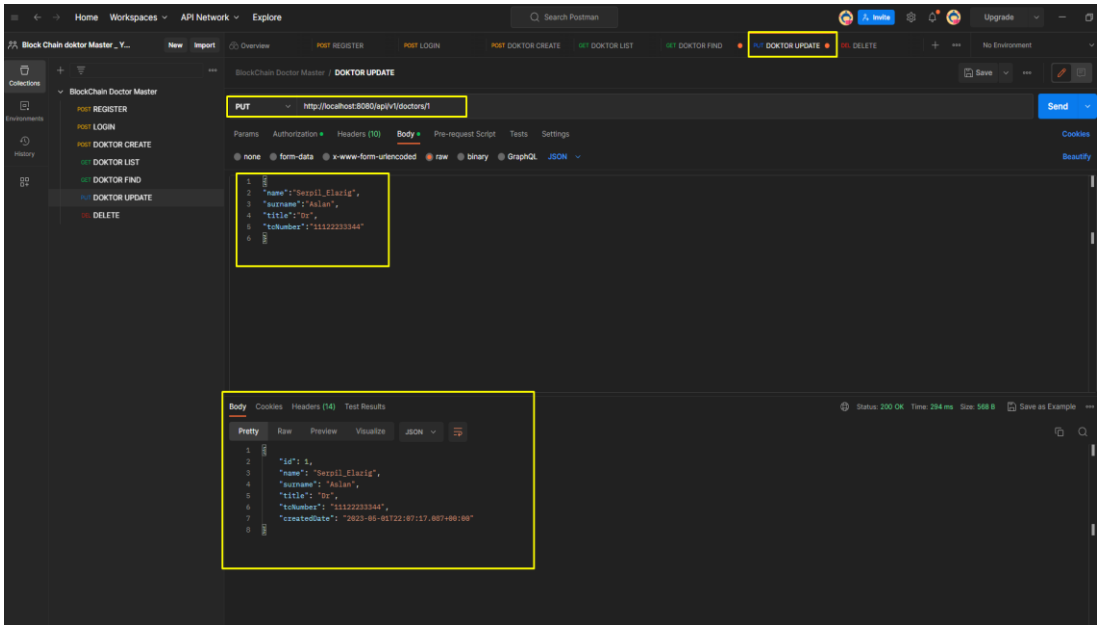
Şekil 3.21. Veri Tabanında Doktor JWT'siz Giriş Yapma Görseli



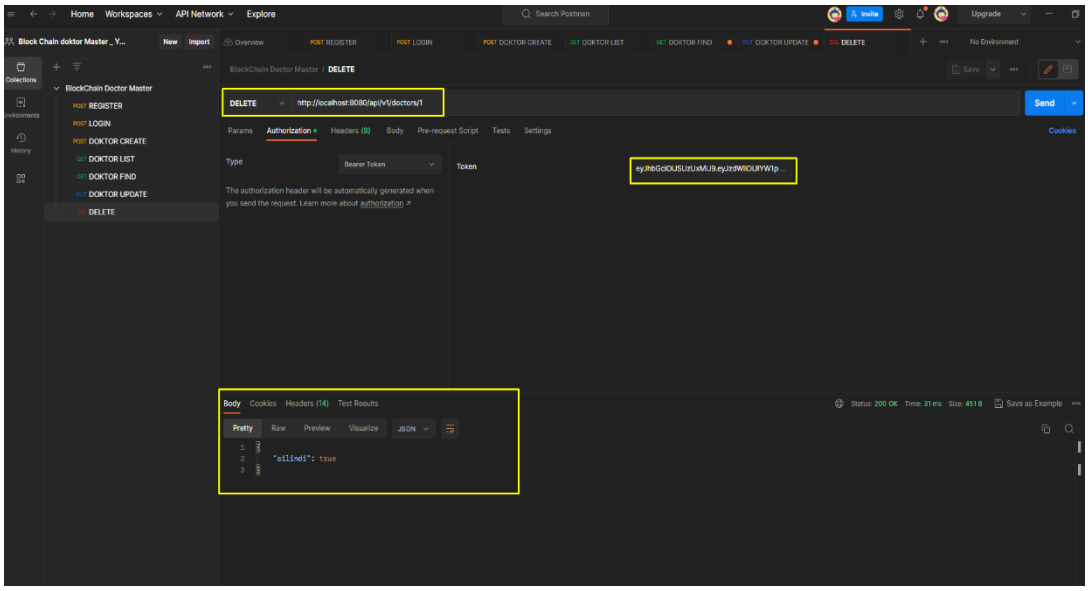
Şekil 3.22. Veri Tabanında Doktor JWT'li Giriş Yapma Görseli



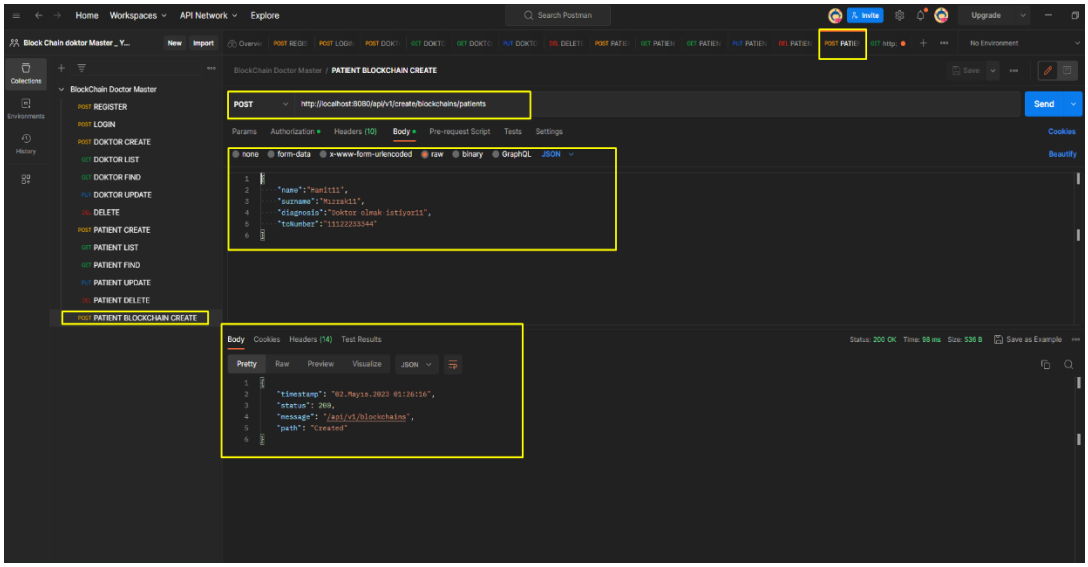
Şekil 3.23. Veri Tabanında Doktor Bulma Görseli



Şekil 3.24. Veri Tabanında Doktor Güncelleme Görseli



Şekil 3.25. Veri Tabanında Doktor Silme Görseli



Şekil 3.26. Veri Tabanında Hasta Silme Görseli

4. ARAŞTIRMA BULGULARI VE TARTIŞMA

4.1. Sağlık Alanında Blok Zincir Teknolojisi

Önerilen yöntemle sağlık alanında veri taşınma hızı, veri güvenliği, veri şeffaflığı ve klasik veri tabanı saklama, sistem kullanıcı girişinin veri tabanı, oturum (session) yöntemine yerine JWT daha güvenlidir. Ayrıca, veri tabanı ve sistemi daha az yormaktadır. Blok zincirini kullanarak bulut servis sağlayıcıları arasında bir veri paylaşım modeline ek olarak sisteme güvenli giriş sağlamak ve akıllı sözleşmelerin erişim kontrol mekanizmalarının kullanılmasında veri denetimi daha iyi bir yapı örneği gösterilmektedir.

Sistemin performans analizini sağlamak üzere kodlamayla katmanlı mimari yapısı ve bulut hizmeti sağlayıcıları arasında veri paylaşımına yönelik mevcut son teknoloji çözümlerle karşılaştırılmaktadır. Bulut hizmet sağlayıcıların daha hızlı bilgi alış verişini sağlayacak bir model oluşturup bu veri gizliliği konusunda daha stabil ve risksiz bir yapı örneği sergilemektedir. Sistemde ki yetkilendirme ile hasta bilgi mahremiyetine önem verilmektedir.

4.2. Tartışma

Yapılan uygulamada, hasta bilgi gizli sağlamak adına blok zinciri, Spring Security, bulut bilişim, özet fonksiyonu ve JWT kullanılmaktadır. Blok zinciri destekli sistemimizin her bir modülünün beklendiği gibi çalıştığı sonucuna varılır. Kullanıcılardan bir tanesi Admin, hastane veya doktor sistem tarafından verilen JWT jeton süresi dolarsa veya sisteme giriş bilgileri olmazsa sisteme girilmeyecek ve sistemde yanlış girişlerinin günlüğünü dosyalarını veri tabanı ve log dosyasında kaydedilmektedir. Sisteme yönetici, doktor veya hastane JWT ile oturum açtığında, sistem ekleme, silme, güncelleme, listeleme sayfasına erişilebilir ve doktor veya hastane akıllı sözleşmede tanımlandığı şekilde yerine getirebilir. Hastane dilerse çalışanı olan doktoru, hastasını sisteme ekleyebilir veya bu kullanıcıları askıya alabilmektedir. Hastane hasta bilgilerinin bilgi gizliliği korumakla görevli olup hastane veya doktor hasta bilgilerine ancak hasta izin verdiğinde erişim sağlayabilir ve bunun sonucunda blok zincirine hasta bilgilerini ekleyebilmektedir.

5. SONUÇ VE ÖNERİLER

Blok zinciri, birden fazla blokların ortaklaşa birbirine bağlanarak verilerin güvenli bir şekilde saklanması olayına verilen genel ada denilmektedir. Blok zinciri teknolojisi kullanarak hasta bilgilerinin gizliliğini sağlamak ve uzaktaki bir hastanedeki hastanın bilgisine güvenli bir şekilde erişimini sağlamada kullanılmaktadır. Sağlıkta veri transferi, veri güveliği, verinin dağıtık bir sistemde yönetilme süreci önemli olduğundan bu problemi blok zinciriyle yapılması son derece önemli görülmektedir.

Blok zincir, bulut bilişimde veri depolama ve paylaşımının diğer merkezi güvenlik çözümlerinin tüm zorluklarına bir cevap niteliğindendir. Blok zinciri internetteki veri belgelerinin ve veri güvenliğinde yeni bir paradigması olarak söylenebilir. Bu teknoloji kullanarak hasta bilgilerinin gizliliğini sağlamak ve uzaktaki bir hastanedeki hastanın bilgisine güvenli bir şekilde erişimin yolları araştırarak, blok zincirinin mankjtığı çerçevesinde uygulamalar gösterilmektedir. Sağlıkta veri transferi, veri güveliği, verinin dağıtık bir sistemde yönetilme süreci önemli olduğundan bu problemi blok zinciriyle yapılması son derece önemli bir faktör olduğu söylenebilir. Blok zincir birçok uygulama alanında kullanılması sağlık alanında da veri paylaşımının bütün güvenlik sorunlarını çözmese de kısmi olarak çözebilecek niteliktedir.

Sağlık alanında bulut teknolojisiyle beraber uygulama alanlarında kullanılması veriyi doğru işlemek, veri paylaşımını sağlamak, veriler üzerinde oynama yapılmasını engellemek ve kötü niyetli kimselerin eline geçmeden şeffaf veri paylaşımı sağlanmaktadır.

Blok zincirinde veri şifreleme için özet fonksiyonu algoritmaları kullanarak veri paylaşımının güvenliliği sağlanmaktadır. Verileri bloklar halinde şifreleyerek bir sonraki düğüme bağlanarak düğümleri oluşturmaktadır. Bu blok süreci ve etkileşim ile tüm veriler entegre hale gelmekte ve verileri bütünlük ilkesini gereği değişen en ufak bir bilginin bozulmasıyla diğer düğümleri etkiyeceğinden dolayı bloklar çalışmaz hale gelmektedir.

Bu çalışmada Java teknolojisi olan JavaEE, Spring boot teknolojisinden yararlanılarak veri kaydetme, veri paylaşımının api üzerinden veri paylaşımı için

Spring Rest, veri güvenliğini sağlamak için Spring Security, veri kaydetmek için Spring Data kullanılmaktadır.

Blok zincirinin en önemli özelliği güvenilmeyen taraflar arasında güven köprüsünü kurmaktadır. Öyle ki şimdiden blok zincirinin birçok alanda kullanımı söz konusu olup özellikle sağlık ve dijital alanda yerini şimdiden aldığını gözlenmektedir. Blok zinciri birçok teknolojiyle eşzamanlı olarak çalışmaktadır. Bu teknolojilerde özet fonksiyonu, konsensüs algoritmaları yardımıyla veri güvenliği, veri paylaşımı sağlayabilmektedir.

Blok zincir bilişimde internetin icadı kadar önemli bir teknoloji olup blok zinciri merkezi otoriteyi, veri güvenliliğini, veri paylaşım hızlılığını, veri şeffaflığı gibi özellikleriyle bilişimde yeni bir dönemin habercisi olduğu öngörülmektedir. Blok zincirinin birçok sosyal medyada, basında her geçen gün ismini duymaktayız. Blok zinciri yeni olduğu için gelecek vaat ediyor ve şimdiden dijital alanda yerini almıştır. Gelecek zamanda blok zinciri devletler üzerindeki etkisinden bahsedileceği şüphesiz bir gerçekleşecektir. Blok zinciri birçok alanda kendisini göstermeye başlamıştır. Bu alanların başında sağlık gelmektedir. Sağlık alanında veri transferi, veri güveliği, verinin dağıtık bir sistemde yönetilme süreci sağlanmıştır. Blok zincirinin zamanda yapay zeka yardımıyla da daha stabil bir sistem olacağından bahsedilmektedir.

6. KAYNAKLAR

[1] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health information science and systems, 2, 1-10.

[2] Krumholz, H. M., & Waldstreicher, J. (2016). The Yale Open Data Access (YODA) project--a mechanism for data sharing. The New England journal of medicine, 375(5), 403-405.

[3] Taichman, D. B., Backus, J., Baethge, C., Bauchner, H., De Leeuw, P. W., Drazen, J. M., ... & Wu, S. (2016). Sharing clinical trial data: a proposal from the International Committee of Medical Journal Editors. Annals of internal medicine, 164(7), 505-506.

[4] Longo, D. L., & Drazen, J. M. (2016). Data sharing. New England Journal of Medicine, 374(3), 276-277.

[5] Fernandes, L. M., O'Connor, M., & Weaver, V. (2012). Big data, bigger outcomes. Journal of AHIMA, 83(10), 38-43.

[6] Grozev, N., & Buyya, R. (2014). Inter-Cloud architectures and application brokering: taxonomy and survey. Software: Practice and Experience, 44(3), 369-390.

[7] UNC (2013) Healthcare relies on "Analytics to better manage medical data and improve patient care" IBM.

[8] Burghard, C. (2012). Big data and analytics key to accountable care success. IDC health insights, 1, 1-9.

[9] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.

[10] Begoyan, A. (2007). An overview of interoperability standards for electronic health records. USA: society for design and process science.

[11] Begoyan, A. (2007). An overview of interoperability standards for electronic health records. USA: society for design and process science.

[12] J. Menezes, P. C. Oorschot, S. A. Vanstone, (1996),Handbook of Applied Cryptography

[13] İnternet: H. Kakavand, N. Kost De Sevres, B. Chilton, The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies, https://ssrn.com/abstract=2849251, 03.01.2019.

[14] I. C. Lin, T. C. Liao, "A Survey of Blockchain Security Issues and Challenges", IJ Network Security, 19(5), 653-659, 2017

[15] Mustafa TANRIVERDİ, Mevlüt UYSAL, Mutlu Tahsin ÜSTÜNDAĞ (2019) Blok zinciri Teknolojisi Nedir ? Ne Değildir ?: Alanyazın İncelemesi

[16] Sevda Çağında, Selçuk Topal (2020) Proof of Meet Konsensüs Protokolünün Gıda TaşımacılığıÜzerine Bir Uygulaması

[17] Hacı Hasan Okuyucu (2020) HASH FONKSİYONLARININ ADLİ BİLİŞİMDEUYGULAMALARI ve C++ İLE ŞİFRELEMEALGORİTMASI TASARIMI

[18] İnternet: T. Wan, H. Max, Bitcoin: Fact. Fiction. Future, https://www2.deloitte. com/insights/us/en/topics/emerging- technologies/bitcoin-fact-fiction-future. html, 04.01.2019

[19] Ömer Kasım (2019) Blok Zinciri Mimarisi ile Elektronik Tıp Kayıtlarının Modellenmesi Üzerine Bir Araştırma Gümüşhane Üniversitesi Fen Bilimleri Enstitüsü Dergisi, pp. 35-42.

[20] Mehmet Aydar(2020.),Salih Cemil Çetin "Blok zincir Teknolojisinin Sağlık Bilgi Sistemlerinde Kullanımı» Avrupa Bilim ve Teknoloji Dergisi, pp. 533-538.

[21] Büşra Özdenizci(2021) Köse, "Sağlıkta Blok Zincir", pp. 368-397.

[22] Talha Murathan, Fatih Murathan(2019) Spor Sektöründe Blok Zincir Uygulamaları" Dergi Park Dergisi, pp. 64-74.

[23] Sreejesh Bhattarai(2015) "Blokchain Teknology For Healtcare Sector» Oulu University Of Applied Sciences, pp. 3-40.

[24] Emre Şafak, Çağlar Arslan,Mesut Gözütok(2020) "Covid-19 Salgınıyla Beklenen Değişimlere Blok Zinciri Teknolojisinin Etkileri» Conferences.

[25] Talha Murathan, Fatih Murathan(2018) "Spor Sektöründe Blok Zincir Uygulamaları» Conferences.

[26] Mukesh Soni, Dileep Kumar Singh(2021) "Blockchain-based security & privacy for biomedical and healthcare information exchange systems» materials today.

[27] Luca Brunese, Francesco Mercaldo, Alfonso Reginelli, Antonella Santone (2019) A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods, Procedia Computer Science,, Pages 1787-1794.

[28] Ashish Sharma, Rahul Singh, Tanwar YashSingh, Ajay Sharma, Shaktiraj Daudra, Gaurav Singal, Thippa Reddy Gadekallu, Sidharth Pancholi(2022) Heart rate and blood pressure measurement based on photoplethysmogram signal using fast Fourier transform July , 108057.

[29] Distributed Hash Tables (DHTs) [WWW Document], n.d. URL https://docs.ipfs.io/concepts/dht/ (accessed 6.20.21).