İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BLOCKCHAİN İLE GÜVENLİ ELEKTRONİK SAĞLIK SİSTEMİ

YÜKSEK LİSANS TEZİ

Mehmet MURAT

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BLOCKCHAİN İLE GÜVENLİ ELEKTRONİK SAĞLIK SİSTEMİ

YÜKSEK LİSANS TEZİ

Mehmet MURAT
(707141006)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Doç. Dr. Enver ÖZDEMİR

Haziran 2018

İTÜ, Bilişim Enstitüsü'nün 707141006 numaralı Yüksek Lisans Öğrencisi Mehmet MURAT, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "BLOCKCHAİN İLE GÜVENLİ ELEKTRONİK SAĞLIK SİSTEMİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Enver ÖZDEMİR** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Oğuzhan KÜLEKÇİ** İstanbul Teknik Üniversitesi	.....
	Yrd. Doç. Dr. Elif SEGAH ÖZTAŞ Karamanoğlu MehmetBey Üniversitesi	.....
	Doç. Dr. Enver ÖZDEMİR İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : 4 Mayıs 2018
Savunma Tarihi : 5 Haziran 2018

Eşime, aileme ve arkadaşlarıma,

ÖNSÖZ

Yüksek lisans eğitimim ve tez süresi boyunca hiçbir konuda yardımını esirgemeyen danışmanım Doç.Dr. Enver Özdemir'e çok teşekkür ederim.

Zorlu ve uzun bir maraton olan yüksek lisans eğitimi süresince beni destekleyen yöneticilerime, arkadaşlarıma, aileme ve eşime destekleri için teşekkür ederim.

Mayıs 2018 Mehmet Murat

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

BLOCKCHAİN İLE GÜVENLİ ELEKTRONİK SAĞLIK SİSTEMİ

ÖZET

İnternetin icadı ve bilgi teknolojilerindeki gelişmelerle birlikte dijitalleşme insan hayatının her alanına girmiştir. Sağlık sektörü de dijitalleşmenin yaşandığı önemli alanların başında gelir. Dijitalleşme birçok açıdan hizmet ettiği sektöre faydalar sağlarken bir takım zorlukları ve riskleri de beraberinde getirir. Sağlık sektörü gibi kişisel verilerin gizliliğinin ve güvenliğinin kritik öneme sahip olduğu günümüzde merkezi ve güncel bilgi teknolojileri yöntemleri bu risklerin ortadan kaldırılmasında yetersiz kalmaktadır.

Yeni ve gün geçtikçe popüler hale gelen blockchain teknolojisi klasik merkezi bilişim sistemlerinin sunduğu hizmetleri kökünden değiştirecek özellikler sunmaktadır. Blockchain kavramı daha çok dijital para birimleri ile aynı olarak görülse de aslında dijital para birimlerinin arkasındaki teknolojik altyapıdır. Blockchain'in sahip olduğu potansiyel dijital para birimlerinin çok daha ötesindedir. Bu teknolojinin potansiyeli fark edilip finans dışı uygulamalarda da kullanılabileceği fikrinin gündeme gelmesiyle birçok sektörden araştırmacılar uygun kullanım senaryoları üzerinde çalışmaya başlamışlardır. Bu sektörlerden birisi de sağlık sektörüdür. Blockchain teknolojisi ile birlikte gelen bu özelliklerden faydalanarak bu çalışma kapsamında güvenli bir elektronik sağlık sistemi altyapısının nasıl olması gerektiği ele alınmıştır.

Bu çalışmanın ilk bölümünde blockchain teknolojisinin temel özellikleri ve tarihi gelişimi hakkında bilgiler verildikten sonra devam eden bölümlerde blockchain teknolojisinin mimarisi, sahip olduğu bileşenler, kriptografik altyapılar ve süreçler teknik açıdan ayrıntılı şekilde ele alınmıştır.

Elektronik sağlık sistemlerinin ele alındığı bölümde güncel sistemlerin yapısı incelenerek sağlanması gereken güvenlik standartları incelenmiştir. Elektronik sağlık sistemlerinin sahip olduğu başlıca sorunlar ele alınarak Avrupa ve Amerika'da yapılmış bazı araştırma ve anket sonuçlarına yer verilmiştir.

Çalışma kapsamında Etherum blockchain teknolojisi kullanılarak web tabanlı dağıtık bir elektronik sağlık uygulaması geliştirilmiştir. Uygulama geliştirilirken html, css, javascript, reactJs gibi web teknolojileri kullanılmıştır. Hastaların elektronik sağlık verilerin şifrelenmiş versiyonları dağıtık veritabanı teknolojisi kullanılarak kayıt altına alınmıştır. Dağıtık veri tabanlarında tutulan verilerin mesaj özü(hash) karşılıkları etherum blockchain sisteminde kurulan özel ağ üzerindeki bloklarda işlem setleri olarak saklanmıştır. Uygulamanın mantıksal iş katmanı solidty dili ile geliştirilen akıllı sözleşmeler aracılığıyla oluşturulmuştur. Uygulamanın teknik ayrıntıları, kullanım senaryoları ve mimari bileşenleri ayrıntılı şekilde ele alınmıştır.

BLOCKCHAIN AND SECURE ELECTRONIC HEALTHCARE SYSTEM

SUMMARY

Medical science is an important scientific field for many centuries. Health is the first priority for humanity since the first days of humankind. Millions of people get treatment in the whole world in every year. Treatment methods and medical devicesare improved with advancing technology. Information technology also made a big contribution to medical science in many aspects in recent years. A new term "e-Health" is created with using computers and mobile devices in healthcare systems. These technological advancements enhance healthcare services in many ways but it comes with new problems such as security and patient privacy.

All sectors which use information and telecommunication technologies (IT) like computers, internet and smart phones have certain security weaknesses. This situation comes with IT nature because each device which is connected to internet can be hacked and informations transferred via internet can be stolen. When it comes with health informations, the security of it becomes more important. Growing use of mobile devices to capture and exchange electronic health information resents complex security and confidentiality problems. Main causes of security weaknesses can be listed as; inadequately configured legal system, defective safeguards by healthcare providers and negligent technical system design. Security in e-health can be examined in two main categories; legal framework and technical security. Legal framework issues can be handled by the legislators and goverments. On the other hand technological data privacy problems can be solved with the help of new distributed technologies like Blockchain.

Blockchain technology can be described as distributed and immutable public ledger which consist of transactions that added by blockchain users and nodes. All transactions in the blockchain network stored in blocks with their hash values and every block connected to previous block with the hash of their header. These connected blocks form a chain where the name, blockchain, comes.. Every transaction in public ledger must be confirmed with blockchain nodes. After a transaction confirmed by independent blockchain nodes, the transaction is persistently added on public ledger. Blockchain technology provides data integrity as it doesn't allow for an update on transaction. In the centralized systems theintegrity of data must be provided by a central authority like companies or institutions despite that in the blockchain system cryptographic functions, decentralized computing systems and public ledger ensure the data integrity.

Data integrity in electronic healthcare systems can be solved by blockchain technology. The other important concern about the electronich health records is the data privacy. Blockchain technology is transparent and transactions can be read by everyone. To Solve this problem, a centralized IT systems and blockchain technology should be combined. A central authority is considered as cryptographic key and identity provider. These keys used for encryption and decryption of electronic health information on blockchain transactions. Patients and other users in e-health system are

registered by the central authority and get the unique identities and key pairs. When the patient creates a health record patient can control his/her own data privacy properties. The owner can decide whether the data should be shared with someone or not.

With the development of blockchain technology a new concept DApp (Decentralized applications) is emerged in software development sector. An application should have some features to be called as DApp. First of all, a business logic must be developed on smart contracts and should not have dependency any backend server or web services. Smart contract transactions executed on blockchain network nodes and execution results also stored in these nodes. User interfaces should connect to blockchain enviroment directly using some frameworks like web3.js in the DApp software architecture. Helper frameworks help communication between smart contracts and user interfaces. There are some platforms like etherum, hyperledger and corda for developing decentralized applications. Software developers can use these platforms to develop their decentralized applications. Storing big size informations in blockchain is very expensive therefore some distributed storage solutions can be used in decentralized applications.

In this thesis, a decentralized electronic health application is developed using Etherum blockchain technology. Truffle is used to create local private etherum network and node. Truffle is a framework for creating and managing etherum networks, migrations and deployments. Smart contracts is compiled and migrated using Truffle. Also Ganache framework used for managing accounts, private keys and monitoring blockchain network. Ganache and Truffle are configured according their white papers to communicate each others.

Patients' and doctors' public informations, hash of electronic health records, data sharing options and other metadata are stored in etherum blockchain. Blockchain is a public ledger technology and all records are readable by everyone so critical informations should not be stored in blockchain. To solve this problem IPFS is used. IPFS (InterPlanetary File System) is a distributed file storage technology used to store encrypted electronic health records. IPFS can be described as a distributed file storage which returns calculated hash values of uploaded file. Electronic health records are stored in this IPFS system and hash of this documents stored in blockchain network.

Business logic layer is developed on blockchain with smart contracts using solidity. Solidity is the programing language of the etherum blockchain platform which has similar javascript notations. Remix online solidity editor used when the coding the business layer. Smart contract functions developed based on application use cases which are creating doctor account, creating patient account, uploading patient electronic data, requesting patient data sharing permissions, patient replaying sharing requests, doctor viewing patient data.

User interface is developed as a web project and html, css, javascript, jquery technologies are used in development process. Metamask is a browser based etherum wallet and it is used for user authentication. It can be installed as a browser addition. When the system admin create a doctor or patient account, he or she assigns an etherum account to this new user and shares the private key of the account. Newly created user imports this private key to metamask wallet and call the electronic healt system web address. Metamask inject the web3.js provider object to web site environment and authenticate the user account. Metamask sign the transactions with this imported private key so miners can verify the transactions by signer account public keys. Also

all accounts public keys stored in blockchain and if any doctor would like to view a patient electronic health record, the doctor sends a sharing request to patient. Patient can view this requests on “my health” records screen and approve/disapprove the requests. If a patient allows the informations, firstly it is encrypted with the doctor’s public key then uploaded to IPFS. IPFS calculates the hash of encrypted document and returns. Returned hash value stored in the blockchain. Finally web application gets the hash value of electronic document from the blockchain and calls the encrypted document from IPFS by this hash value when the doctor visits the patient health records page. Then encrypted file is decrypted by doctor private key. After all this process doctor can view the patient informations.

1. GİRİŞ

Blockchain teknolojisi geçmişe dönük değişiklik yapılamayan büyük bir kayıt defteri olarak düşünülebilir[1]. Bu defter içerisindeki kayıtlar eskiye dönük değiştirilemez ve sisteme dâhil olan tüm katılımcılarda aynı defter bulunur. Yeni bir işlem gerçekleştiğinde bu iş sistemdeki tüm defterlere ortak bir mutabakat sonucu silinmemek üzere eklenir. Merkezi bir otoriteye ihtiyaç duymadan verinin bütünlüğünün ve gizliliğinin sağlandığı bu sistem özellikleri açısından birçok sektörde potansiyel uygulama alanına sahiptir.

Blockchain teknolojisi ilk defa hayatımıza 2008 yılında bitcoin ile girmiştir[2]. Bir grup insanın kendi aralarında banka gibi merkezi bir otoriteye ihtiyaç duymadan para transferi yapma ihtiyacı bu teknolojinin ortaya çıkmasına sebep olmuştur. Günümüzde çok popüler olan kripto paraların temeli böyle atılmıştır. Sisteme dâhil olan kişiler arasındaki para transferi işlemlerinin geçerliliğinin kontrolleri ve kontroller sonrası tüm katılımcıların kayıt defterlerine eklenmesi sistemin güvenirliliğini sağlamaktadır. Blockchain içeresindeki bu teknolojik yaklaşımlar paranın güvenliğini bankalardan alarak teknolojik altyapılara ve kriptografik zor matematiksel problemlere devretmektedir. Kripto para dünyasında blockchain üzerinden sadece parasal değerlerin transferi yapılırken blockchainin sahip olduğu potansiyel bunun çok daha ötesindedir. Blockchain ile her türlü veri yapısının saklanıp transfer edilebileceği fikri teknolojinin son yıllarda daha da popüler hale gelmesine sebep olmuştur. Farklı sektörlerden uzmanlar, mühendisler, akademisyenler ve şirket sahipleri blockchain teknolojisine ilgi göstermekte ve teknolojinin araştırılıp uygulanması için çeşitli çalışmalar yapmaktadır. Bu sektörler içerisinde bankacılık, finans, sigorta, emlak, sağlık, hizmet gibi birçok alan sayılabilir.

1.1 Blockchain Tarihi

Blockchain teknolojisinin temelini oluşturan fikir ilk defa 1991 yılında dijital olarak imzalanmış belgelerin geçmişe yönelik değiştirilememesi projesiyle ortaya çıkmıştır[3]. Temel fikrin gerçeğe dönüşmesi 2008 yılında kişiler arası dijital para

transferinin yapılmasını sağlayan Bitcoin projesiyle gerçekleşmiştir. Satashi Nakamoto takma adıyla yayınlanan makale ile Bitcoin ve arkasındaki teknoloji tüm dünyaya duyurulmuştur[2]. Blockchain teknolojisi kullanılarak geliştirilmiş olan ilk uygulama olması açısından Bitcoin yıllarca blockchain ile özdeşleştirilmiştir, ayrıca kullanıcı sayısı ve bilinirliği düşünüldüğünde bu teknolojiyi kullanan en büyük ve en başarılı uygulamadır.

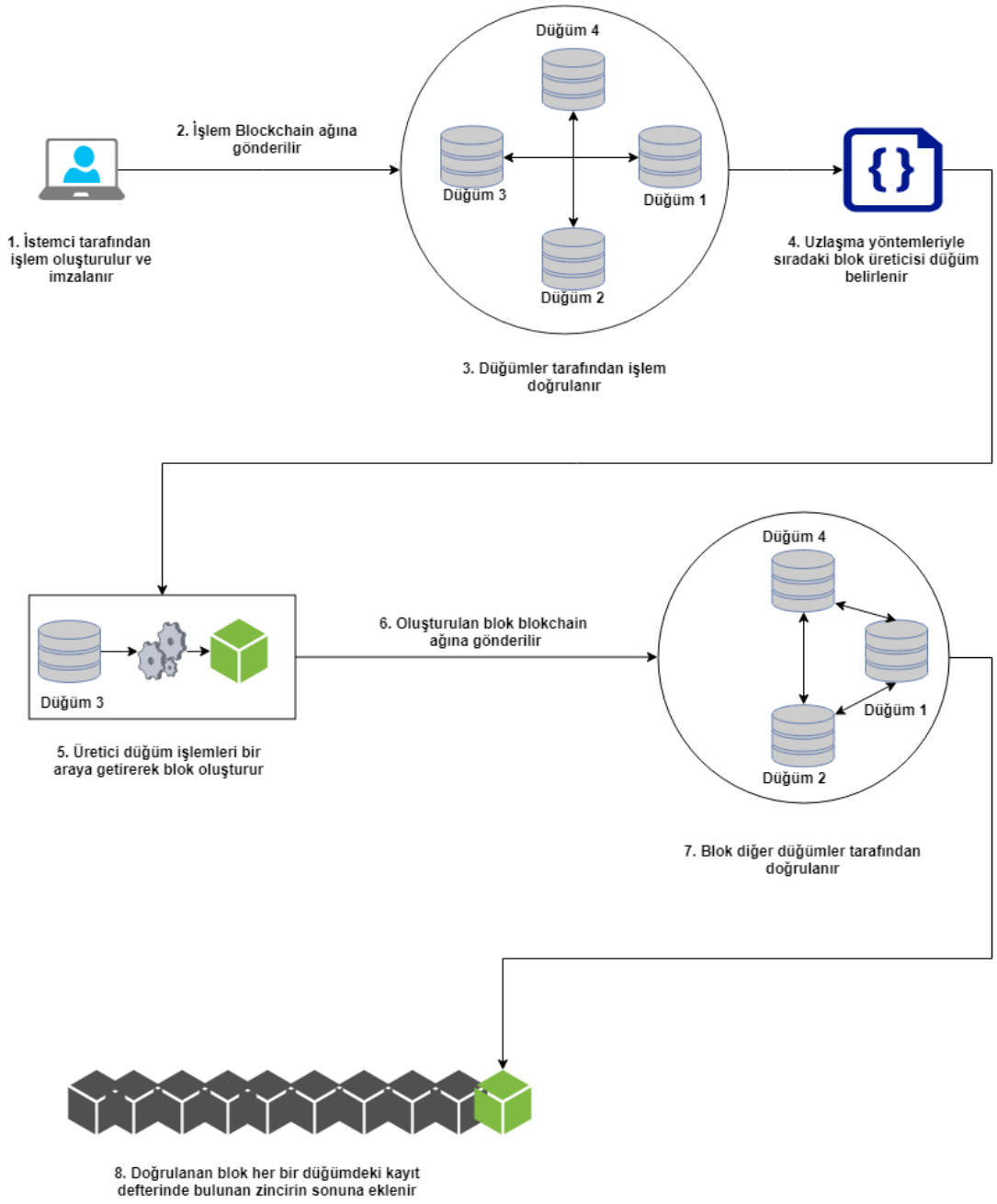
Bitcoin öncesinde birçok dijital ödeme sistemi bulunmaktaydı fakat hiç birinin kullanımı geniş kitlelere ulaşamamıştı. Blockchain teknolojisinin kullanılması Bitcoin sisteminin dağıtık bir yapıda üçüncü kişilere ihtiyaç duymadan dijital para biriminin yönetilmesine olanak sağladı. Bunun getirdiği en büyük fayda ise kişiler arası parasal işlemlerin merkezi bir otoriteye ihtiyaç duymadan doğrudan yapılabilmesiydi[4].

Merkezi bir otorite olmadığı için blockchain tabanlı bu sistemlerde blockchain ağının bakımı, yeni eklenen işlemlerin doğrulanması ve bu işlemlerin bloklara eklenmesi madenciler tarafından yapılmaktadır. Yüksek işlemci gücü gerektiren ve fazla miktarda enerji tüketen cihazlarla yapılan bu işlemlerin maliyetleri de oldukça yüksektir. Blockchain teknolojisi madencilerin sisteme dahil olması ve bu maliyetleri göze alacak şekilde sistemde kalmaları için ödül sistemine dayalı konsensüs mekanizmalarını içerir. Bu konsensüs mekanizmalarında madenciler hem çözdükleri kriptografik matematiksel problemler başına ödül alırken hem de sisteme yeni eklenecek işlemleri doğrulayarak sistemin veri bütünlüğünün korunmasını sağlarlar. Kripto para dünyasında blockchain sahip olduğu bu doğrulama yöntemi ile çift harcama hatalarının tamamen önüne geçmektedir. Blockchain teknolojisinin bir diğer ilginç özelliği ise herkese açık şekilde tüm işlemler görüntülenebilirken aynı zamanda anonimliğin korunabilmesidir. Bir işlemin hangi hesaptan yapıldığı belli iken o hesabın kime ait olduğu bilinmemektedir. Ayrıca hesaplar yaratılırken kişisel hiçbir bilgi alınmamakta şifre karşılığı tek bir public key kullanıcıya adres olarak verilmektedir. Böylece büyük ölçüde hem anonimlik korunmuş olup hem de şeffaflık sağlanmaktadır.

2. BLOCKCHAİN MİMARİSİ

Blockchain bir çok insan tarafından aşırı kompleks olarak düşünülse de blockchain mimarisi bilişim, kriptografi ve finans gibi farklı alanlarda daha önceden de kullanılan ve gayet iyi bilinen bir takım bileşenlerden oluşmaktadır. Mimari incelendiğinde kriptografi alanından asimetrik şifreleme, imzalama ve özetlemenin kullanıldığı görülür. Mimari içerisinde yeralan bir diğer bileşen ise dağıtık ağ yapısıdır. Dağıtık ağ yapısının bilişim dünyasındaki yeri blockchainden öncesine dayanır. Finans sektöründe hesaplama işlemleri için yüzyıllardır kullanılan kayıt defteri kavramı blockchainde yerini alan bir diğer önemli bileşendir. Tüm bileşenlerin parça parça ele alınması hem teknolojinin daha kolay şekilde kavranmasını hem de uygun iş modellerinde hayata geçmesini daha kolay hale getirecektir. Arka planı bilinmeyen bir teknolojiden fayda sağlayabilme fikri çok da makul bir düşünce olarak görülemez. Tüm bu açılardan ele alındığından blockchain mimarisine hâkim olmanın teknolojiyi kullanma ve değişen dünyaya ayak uydurma açısından ne denli önemli olduğu görülebilir.

Blockchain mimarisi şekil 2.1'de gösterilmiştir. İstemcinin sahip olduğu saklı anahtarla işlem yaratılıp imzalanarak blockchain ağına gönderilir. Gönderilen bu işlem doğrulanmamış işlemler havuzunda doğrulanmak üzere bekletilir. Blockchain ağındaki düğümler bu işlemleri doğrulayarak bir sonraki blok içerisine eklerler. Bir sonraki bloğun hangi düğüm tarafından yayınlanacağı ağ genelindeki uzlaşma yöntemleriyle belirlenir. Yayıncı düğümün ürettiği blok diğer düğümler tarafından doğrulanır ve blockchain kayıt defterlerindeki zincirin son halkası olarak eklenir. Mimarinin bileşenleri devam eden bölümlerde ayrıntılı olarak ele alınmıştır.



Şekil 2.1: Blockchain mimarisi

2.1 Özetleme Fonksiyonları

Blockchain teknolojisi içerisindeki akışların önemli bir kısmında birçok kriptografik fonksiyondan faydalanılır. Bunlardan bir tanesi de özetleme fonksiyonlarıdır. Kriptografik bir özetleme fonksiyonu aldığı değişken uzunluktaki mesajlara karşılık sabit uzunlukta çıktılar üretir. Örneğin çok uzun bir makele ile tek kelimeden oluşan bir girdinin üreteceği çıktının uzunluğu özetleme fonksiyonlarında aynıdır. Bir

fonksiyonun kriptografik özetleme fonksiyonu olabilmesi için sağlaması gereken bazı özellikler vardır:

1. Verilen bir mesaj m için fonksiyon çıktısı h(m) hızlı bir şekilde hesaplanabilmelidir
2. Özetleme fonksiyonu tek yönlü olmalıdır yani bilinen bir özet çıktısını sağlayan bir girdiyi hesaplamak mümkün olmamalıdır.
3. Verilen iki farklı mesaj m1 ve m2 için aynı özet çıktısının bulunabilmesi hesaplama süresi açısından mümkün olmamalıdır[5].

Şekil 2.2: Örnek bir özetleme fonksiyonu.

Kriptografi dünyasında MD5, SHA-1, SHA-2, SHA-3, BLAKE birçok farkli hash algoritması bulunmaktadır. Blockchain teknolojisi içerisindeki süreçlerde ihtiyaç duyulan kısımlarda SHA-256 algoritması kullanılmaktadır. SHA-256 algoritması SHA-2 algoritmasının bir alt koludur. Bu fonksiyon verilen mesajlar için 256 bitlik çıktılar üretir. 256 bitlik çıktılar olması bu algoritmanın 2^{256} farklı fonksiyon çıktısı üretebildiğini göstermektedir. Rakamsal olarak düşünüldüğünde 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 gibi büyük bir sayı elde edilmektedir. Böyle büyük bir havuzda çakışma elde etmek için en az 2^{128} deneme yapılması gerekir. Bu deneme sayısı güncel bilgisayarların işlemci kapasitesiyle imkânsızdır. Blockchain adı teknolojinin içerisinde yer alan zincir şeklindeki bloklardan gelmektedir. Bu bloklar içerisinde blockchain ağındaki işlemler yer alır ve her bir blok bir öncekine referansla bağlıdır. Her bir blok içeriği sha-256 algoritmasıyla özetlenir. Ayrıca blokların içerisinde kendisinden önceki bloğun başlık kısmındaki bilgilerin hash değeri bulunur. Başlıkların hashlenmesinde de SHA-256 algoritması kullanılmaktadır.

2.2 İşlemler

Blockchain ağında katılımcılar arasındaki varlık transferlerinin kayıtlarına işlem denir. Bu işlemler bloklar içerisinde saklanır. Her bir blok birden çok işlemden meydana

gelir. Bir işlemin yapısı incelendiğinde birden fazla kısımdan oluştuğu görülmektedir. Farklı blokchain teknolojilerinde bu alanlara ek başka alanlarda gelebilir. Temel olarak bir işlem aşağıdaki alanları içerir:

1. Toplam Miktar: Transfer edilecek dijital varlıkların toplam miktarıdır. Kripto para miktarının toplamını temsil edebileceği gibi kayıt defterine eklenecek başka varlıkların toplamını da temsil edebilir.

2. Girdi Listesi: Transfer edilecek varlıkların listesidir. Gönderici hesap adresiyle birlikte miktarlar yer alır. Miktarların toplamı toplam miktar alanındaki değere eşittir.

3. Çıktı Listesi: Transfer edilecek varlıkların miktarları ve alıcı adresleriyle yeni sahiplerinin listesidir.

4. Hash Değeri: İşlem içeriğinin hash değeridir. Bu işlemi temsilen bazı blockchain teknolojilerinde hash yerine özgül id kullanılır.

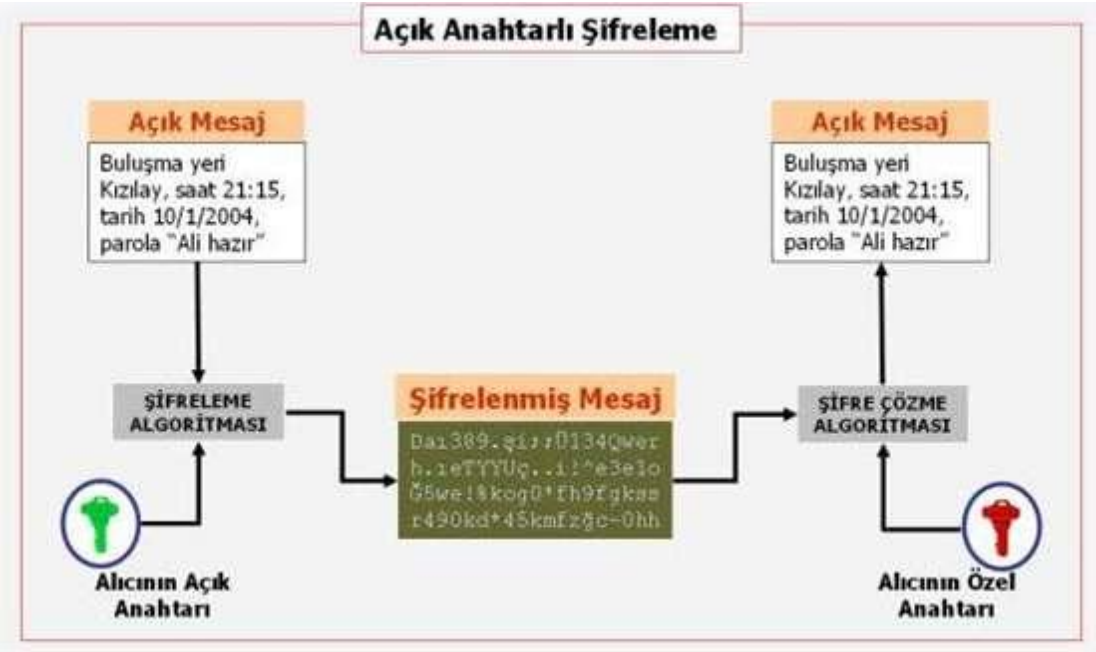
Blockchain teknolojisinde işlemlerin doğrulanması açık anahtarlı kriptografik algortimalar ile sağlanır. Saklı anahtar ile imzalanmış işlemler göndericinin açık anahtarı kullanılarak doğrulanır.

2.3 Açık Anahtarlı Kriptografik Algoritmalar

Açık anahtarlı kriptografik algoritmalar ilk defa 1970'li yıllarda ortaya çıkmıştır ve kriptografi dünyasında devrim niteliğinde bir değişikliğe sebep olmuştur. Simetrik şifreleme algoritmalarında kullanılan anahtarın şifreleme öncesi güvenli bir kanaldan paylaşılması zorunluluğu birçok kullanım senaryosunda büyük problemlere sebep olmaktaydı. Özellikle birbirinden uzak ve böyle güvenli bir kanala sahip olmayan katılımcılar arasındaki şifreleme problemine açık anahtarlı kriptografi çözüm getirmiştir. Açık anahtarlı algoritmalar birisi herkes tarafından bilinen açık bir anahtar ile diğeri sadece sahibi tarafından bilinen saklı anahtar çiftinden meydana gelir. Açık olan anahtarla yapılan bir şifreleme sadece saklı olan anahtar ile çözülebilir. Açık anahtar ile gizli anahtar arasındaki ilişki çözümü hesaplama gücü açısından mümkün olmayan zor matematiksel problemlere dayanır. En popüler açık anahtarlı şifreleme algoritmaları olarak RSA, ElGamal ve NTRU gösterilebilir.

Açık anahtarlı kriptografi temel olarak iki amaç için kullanılır. Bunlardan bir tanesi mesajın açık olan anahtar ile şifrelenip saklı olan anahtar ile çözülmesidir. Bu kullanım

tipinde mesajı gönderen kişi alıcının açık anahtarı ile mesajı şifreler alıcı kendi saklı anahtarı ile şifreyi çözer ve mesajı elde eder. Şekil 2.2'de açık anahtarlı bir şifreleme örneğine yer verilmiştir.



Şekil 2.3: Açık anahtarlı şifreleme[6].

Asimetrik kriptografinin diğer kullanım alanı ise imzalamadır. İmzalama bir mesajın gerçekten o göndericiden gelip gelmediğinin kontrolü amacıyla kullanılır. Gönderici kendinde bulunan saklı anahtar ile mesajı imzalar ve alıcıya gönderir. Alıcı ise göndericinin açık anahtarını kullanarak bu imzayı doğrular. İmzanın doğrulanabiliyor olması göndericinin kimliğinin doğrulanmasını sağlar.

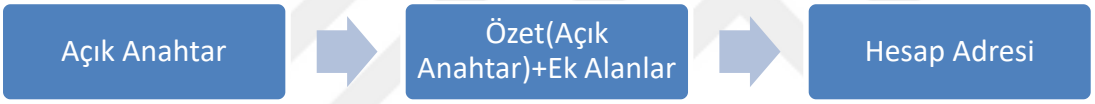
Blockchain teknolojisi içerisinde asimetrik kriptografinin kullanım alanları şöyle sıralanabilir:

- İşlemlerin saklı anahtar ile imzalanması
- Hesap adreslerinin açık anahtarlar ile türetilmesi
- Saklı anahtar ile imzalanmış işlemlerin açık anahtarla doğrulanması

2.4 Hesap Adresleri

Blockchain teknolojilerinde ortak yapılardan bir tanesi de hesaplar ve bu hesapların adresleridir. Sisteme dâhil olan her yeni kullanıcı için yeni bir adres üretilir. Bu adres bankacılık dünyasındaki IBAN olarak düşünülebilir aynı zamanda adresler blockchain

sistemine dâhil olan kullanıcıların kimlikleri niteliğindedir. Dijital varlıkların transferinde varlığın kimler arasında el değiştireceği bilgisi bu hesap adresleri üzerinden anlaşılabilir. Blockchainde yer alan bir işlemde "Kimden" ve "Kime" alanları gönderici ve alıcının adres bilgilerinden oluşur. Bu adresler anlamsız alfa numerik karakterlerden meydana gelir ve çoğu zaman akılda tutması zordur. Adreslerin kullanımı kolaylaştırmak açısından QR kod tarzı yardımcı uygulamalar kullanılabilmektedir. Adreslerin üretilmesinde kullanıcıya ait açık anahtarlar kullanılır. Açık anahtarların özet değerinin alınıp ekstra alanların eklenmesiyle bir blockchain adresi elde edilmiş olur. Dijital bir varlığın sahiplik bilgisi bu adreslere tanımlıdır. Bir kullanıcının sahip olduğu dijital varlık üzerinde işlem yapabilmesi içinse o hesaba ait saklı anahtara sahip olması gerekir. Çünkü bu dijital varlığın harcanması için yaratılacak olan işlemin kullanıcının saklı anahtarı ile imzalanmış olması gerekmektedir. Yaratılan bu işlemin doğrulanmasında hesap adresinin türetildiği açık anahtar kullanılmaktadır. Hesap adresinin elde edilme akışına şekil 2.4'te yer verilmiştir.



Şekil 2.4: Hesap adresi elde etme.

2.5 Cüzdan

Kullanıcıların saklı anahtarları büyük öneme sahiptir. Dijital varlıkların güvenliği için bu anahtarın çok sağlam ve güvenli bir şekilde saklanması gerekmektedir. Bu anahtarların saklandığı uygulamalara cüzdan adı verilir. Bu cüzdanlar yerel diskler üzerinde olabilirken bulut içerisinde de yer alabilir. Kullanıcılar genellikle bu anahtarların gizlenmesiyle ilgili manuel bir şey yapmak zorunda değillerdir. Cüzdan uygulamaları ile hesap adresi yaratılırken bu işlemler otomatik olarak yapılır ve üretilen anahtar güvenli bir şekilde saklanır. Cüzdanlar ayrıca açık anahtarı ve kullanıcıya ait dijital varlık bilgilerini de göstermektedir.

2.6 Kayıt Defteri

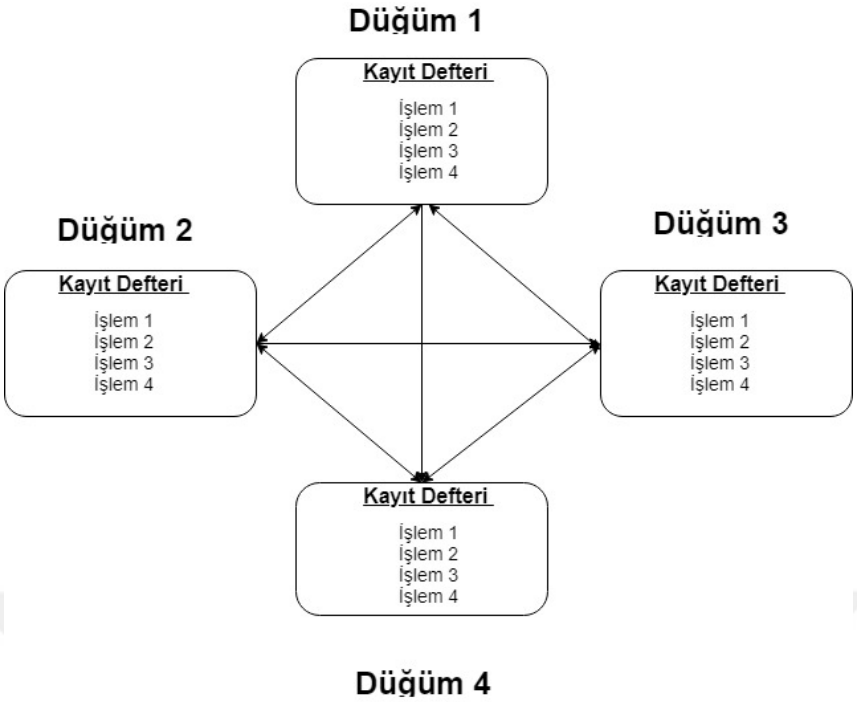
Blockchain teknolojisindeki dağıtık mimari sebebiyle veriler her bir katılımcıda bulunan herkese açık kayıt defterlerinde tutulmaktadır. Bu kayıt defterleri içerisinde

blockchain ağında yaratılmış ve doğrulanmış işlemler yer alır. Bu işlemler dijital varlıkların hangi hesaplar arasında el değiştirdiğini göstermektedir. Bir işlemin bu kayıt defterlerine eklenebilmesi için katılımcılar arasında bulunan uzlaşma algoritmasıyla doğrulanmış olması gerekir. Katılımcıların işlemin geçerliliğiyle alakalı hemfikir olmasından sonra bu işlem ağdaki tüm katılımcıların kayıt defterlerine geri dönülemez şekilde eklenir. Kayıt defterlerindeki bu işlemler eskiye dönük olarak değiştirilemez veya silinemezler. Aynı kayıtlar tüm katılımcılarda olduğu için geçmişe yönelik bir manipülasyon söz konusu olamaz.

Teknolojik gelişmeler öncesi tarih boyunca varlıkların ve işlemlerin takibi tabletler ve yazılı defterler ile yapılmıştır. Bilgisayarın hayatımıza girişi ve dijitalleşme ile birlikte bu süreçler bilgisayar ortamına taşınmıştır. Blockchain teknolojisi ortaya çıkana kadar bu kayıtların saklanması merkezi veri tabanlarında ve sistemlerde gerçekleştirilmiştir. Merkezi sistemlerde bu işlemlerin yapılabilmesi için kullanıcılara güven verebilecek üçüncü şahıslar gerekmektedir. Bu üçüncü şahıslar olarak devletler, bankalar ve finans kuruluşları örnek olarak gösterilebilir. Kullanıcılar bu üçüncü şahıslara ne kadar güvenseler de merkezi bir sistemin olmasından ötürü çeşitli riskler ve dezavantajlar vardır:

- Merkezi bir veri tabanında meydana gelecek arıza veya saldırı durumunda çok kritik bilgiler kaybolabilir veya çalınabilir. Bilgiler tek bir otorite sorumluluğunda olduğu için buradaki verilerin geri dönüşü sadece düzenli yedeklemeyle mümkündür. Yedeklerin alındığı yerler yine merkezi bir yapı olacağı için aynı ihtimaller bu yedekler için de geçerlidir.
- İşlemlerin doğruluğu sadece merkezi üçüncü şahıs tarafından doğrulanmaktadır. Merkezi sistemin yapacağı bir hata tüm hesapların karışmasıyla sonuçlanabilir.
- Geçmiş işlemlerin üzerinde değişiklik yapılmış olabilir. Eğer merkezi bir otorite varsa bu otoritenin yetki verdiği sistem yöneticileri geçmiş işlemler üzerinde değişiklik yapmış olabilirler.

Güvenlik tedbirleri ve çeşitli politikalar ile bu dezavantajlar ve riskler merkezi sistemlerde en aza indirgenebilse de küçük ihtimaller her zaman mevcuttur. Blockchain teknolojisi sahip olduğu özelliklerle bu dezavantajları ve riskleri ortadan kaldırmak için yola çıkmıştır. Şekil 2.5'de kayıt defterlerinin her bir düğümde aynı içerikle olduğu görülebilir.



Şekil 2.5: Blockchain kayıt defteri

2.7 Bloklar

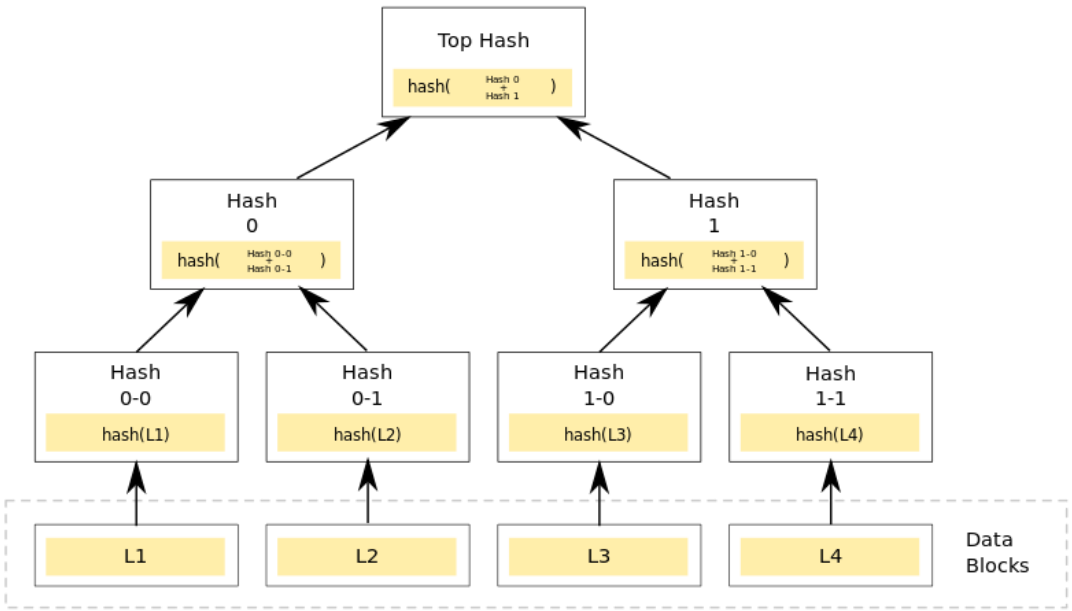
Kullanıcılar bir işlem yaptıklarında blockchain ağındaki düğümlerden birine bu işlemin yaratıldığı bilgisi ulaşır. Bu aşamada işlemin blockchain ağına eklendiği henüz söylenemez. Ağa dâhil olan ve işlemden haberdar olan düğüm diğer düğümleri böyle bir işlemin varlığından haberdar eder. Böyle işlemler bloklara ekleneceği zamana kadara işlem havuzunda bekletilirler. Farklı blockchain teknolojilerinde bu işlemlerin doğrulanması ve bloklara eklenmesi farklı yöntemlerle yapılmaktadır. Madenci olan düğümlerden bir tanesi işlemin geçerliliğini doğrulayarak sıradaki blok içerisine ekler. Diğer düğümler de blok içerisindeki tüm işlemlerin geçerliliğinin kontrolünden sorumludur. Bir blok içeresinde bir işlemin geçersiz olması tüm bloğun geçersiz olmasına sebep olur. Düğümler işlem geçerliliklerini kontrol ederken işlemi yaratan hesapların gerçekten bu dijital imzayı oluşturacak saklı anahtara sahip olup olmadıklarını kontrol ederler. Eğer imza göndericinin açık anahtarı ile doğrulanabiliyorsa bu durum işlem sahibinin gerçekten saklı anahtara sahip olduğunu gösterir. Bir bloğun geçerliliği onaylandıktan sonra bu bloğun hash değeri alınarak diğer düğümler ile de paylaşılır. Blok içerisinde yeralan işlemlerde daha sonradan

yapılacak bir değişiklik bloğun hash değerini değiştireceğinden verinin bütünlüğü bu hash değerinin kıyaslanmasıyla sağlanır. Tüm işlemlerin hash değerlerinin blok başlığında yer alması yerine merkle tree yöntemi kullanılır. Bu yöntem blockchain gibi dağıtık bir yapıda datanın doğrulanması ve geçmişe yönelik değişmezliğinin kontrolü açısından gayet kullanışlıdır.

Bir blok genel olarak aşağıdaki bileşenlerden meydana gelir:

- Blok numarası
- İşlem listesi
- Güncel blok özet değeri
- Önceki blok özet değeri
- Merkle tree root özet değeri
- Zaman damgası
- Tek seferlik anahtar

Şekil 2.6'da Merkle ağacı örneği görülmektedir. Data bloklarının ayrı ayrı hashlerinin saklanması yerine adım adım kombine edilerek tek bir özet hash edilmiştir. Şekilde gösterilen ve en alt satırda yer alan L1-L4 veri blokları blockchain teknolojisinde işlem bilgilerine karşılık gelmektedir.



Şekil 2.6: Merkle ağacı[7]

Bloklar ve Merkle tree arasındaki ilişki şekil 2.7'de gösterilmiştir. Her bir blok temel olarak başlık ve gövde olmak üzere iki kısımdan oluşur. Blok başlıklarında bir önceki bloğun hash değeri, zaman damgası, anlık değişken anahtar ve blok içerisindeki işlemlerin Merkle kök özet değeri bulunur. Bloğun gövde kısmı ise kendi başlık kısmının hash değerinden ve barındırdığı işlemlerden meydana gelir. Blokların zincir şeklinde birbirine bağlanmasını başlık bilgilerinde yer alan bir önceki bloğun başlığının hash değeri sağlamaktadır. Zincirin herhangi bir yerindeki blok başlığında meydana gelecek bir değişme zincirin devamındaki tüm hash değerlerini değiştireceği için bunun tespiti oldukça kolaydır. Bir blok başlığının hash değeri içerisinde merklee root hash değeri de bulunduğundan ötürü herhangi bir bloğun herhangi bir işleminde meydana gelecek bir değişiklik zincirin devamındaki tüm özet değerlerini değişmesine sebep olur.

Şekil 2.7: Merkle ağacı ve blockchain[8]

Tx0,Tx1,Tx2,Tx3 işlemleri blok02'ye aittir. Bu işlemlerin root hash değeri hesaplanarak başlık bilgisinde ilgili yerde saklanmaktadır. İşlemler, bloklar ve Merkle tree arasındaki ilişki açık bir şekilde gösterilmektedir. Merkle ağacı sayesinde blok içerisinde yaralan tüm işlemlerin özet değerleriyle sağlanabilecek verinin bütünlüğü ilkesi tek bir özet ile sağlanabilmektedir.

3. BLOCKCHAIN ÇALIŞMA MEKANİZMASI

Blockchain teknolojisinde merkezi bir otorite bulunmamaktadır. Sistemin sürekliliğini ve bakımını ağa dâhil olan katılımcıların bilgisayarları üstlenmektedir. Her bir katılımcıya düğüm adı verilir. Hangi işlemlerin yeni bloklarda yer alacağı ve hangi blokların üretilerek blockchain zincirine yeni bir halka olarak ekleneceği bu düğümler tarafından belirlenir. Düğümler genel olarak tam ve hafif olmak üzere ikiye ayrılır. Tam düğümler blockchain kayıt defterinin bütün bir kopyasını üzerlerinde barındırır ve sisteme eklenecek yeni aday blokları oluştururlar. Tam düğümler aynı zamanda yeni blokların doğrulanmasından da sorumludurlar ve madenci olarak isimlendirilmektedirler. Hafif düğümler ise kayıt defterinin tüm kopyasını üzerlerinde tutmazlar. Bu tip düğümler genellikle akıllı telefon gibi daha düşük kapasiteli aygıtlar üzerinde yer alır. Hafif düğümler yeni blok yaratılmasında ve doğrulanmasında görev alamazken sisteme yeni işlemlerin eklenmesi operasyonlarında kullanılırlar.

Blockchain ağında zincire yeni eklenecek olan bloklar işlemlerden oluşmaktadır. Sisteme dâhil olan düğümler yeni işlemler yaratabilir. Oluşturulan bu işlemler madenci düğümleri arasında bulunan harcanmamış işlemler havuzunda biriktirilirler. Her madenci bir sonraki bloğu üretmeye aday olabilir. Bloklar üretilirken bu havuzdaki işlemler bloğa dâhil edilir. Hangi işlemlerin bir sonraki blokta bulunacağı hem işlemin yaratılma tarihine hem de işlem için ödenmiş olan masraf bilgisine bağlıdır. Daha eski ama daha düşük masraflı bir işlemle daha yeni ve daha yüksek masraflı bir işlem aynı blokta yer alabilir.

Bloklar yaratılırken madenci düğüm tarafından blok yapısına uygun şekilde tüm hash değerleri oluşturulur ve işlemlerdeki imza bilgilerinin gerçek sahipleri tarafından atılıp atılmadığı kontrol edilir. Daha sonra bu blok diğer madenci düğümler arasında kontrol edilmek üzere yayılır. Kontrol aşamasında diğer düğümler bu bloğun yapısının ve içeriğinin uygunluğu kontrol ederler ve uygun bulunmayan bloklar diğer düğümler tarafında reddedilir. Merkezi bir otorite olmadığı için yeni bloğun hangi madenci tarafından yaratılacağı zor kriptografik bulmacaların çözümüyle belirlenir. Çözüm için

tek seferlik rastgele bir metni tahmin etmeye çalışan madenciler bu değeri bulmak için çok yüksek sayıda deneme yaparlar. Yüksek sayıda yapılan denemeler fazla miktarda işlemci ve elektrik kaynağı gerektirir. Rastgele değişkeni ilk bulan madenci sistem tarafından ödüllendirilir ve bloğu oluşturma hakkı elde eder. Sistemi ayakta tutan ve düğümlerin masraflarını karşılayan şey bu ödül mekanizmasıdır. Madenci tarafından oluşturulan ve işlemleri içeren blok ağ genelindeki diğer düğümlere yayınlanır. Düğümler arası bu kontrol ve blok ekleme mekanizmasına uzlaşma adı verilir. Farklı blockchain sistemlerinde farklı uzlaşma yöntemleri kullanılabilmektedir. Sonraki kısımlarda uzlaşma yöntemleri ayrıntılı şekilde ele alınacaktır.

3.1 Uzlaşma Yöntemleri

Blockchain sistemlerinde merkezi bir otorite bulunmadığı için sistemin devamlılığının sağlanmasında ve süreçlerde çeşitli karışıklıklar yaşanabilmektedir. Yeni bir bloğun hangi düğüm tarafından üretileceği sorusu bu karmaşalardan biri olarak gösterilebilir. Yeni blokların üretilmesine karar verilirken çözülen bulmaca ödül sisteminin de bir parçasıdır. Katılımcılar bu ödülü kazanmak için birbirleriyle büyük bir rekabet içerisindedir. Ödülün kim tarafından alınacağı ve aynı anda farklı düğümler tarafından çözülmüş bulmacalarda kimin ödüllendirileceği problemleri uzlaşma yöntemleriyle çözülmektedir. Bu uzlaşma yöntemleri birbirini hiç tanımayan katılımcıların birbirlerine güvenerek aynı ekosistem içeresinde rekabetçi bir anlayışla çalışmalarına olanak sağlamaktadır.

Sisteme dâhil olan kullanıcılar sistemin sahip olduğu güncel durumu ve sistemde kullanılan uzlaşma yöntemini kabul ederek katıldıkları için ileride çıkacak anlaşmazlıkların kapası kapanmış olur. Blockchain zincirinde ilk blok olan Genesis bloğu hangi uzlaşma yönteminin kullanılacağı barındırmakla birlikte tüm değerleri 0 olan hashler bulundurur. Ayrıca kendisinden önceki blok olmadığı için ilgili alanın hash değeri de 0'dır. Blockchain ağına yapılacak olası saldırılarda sistemde kullanılan uzlaşma yöntemi ile saldırganların ağı ele geçirmesi ve geçersiz blokları zincire eklemesinin de önüne geçilir.

3.1.1 İş ispatı (proof of work) uzlaşma yöntemi

İş ispatı yöntemi hesaplanması zor kriptografik bulmacalara dayanmaktadır ve Bitcoin blokchain ağında bu yöntem kullanılmaktadır. Yeni üretilecek bloğun kim tarafında

üretileceğine bu yöntemle karar verilir. Adından da anlaşılacağı üzere blok üretmek için bir çaba harcandığının ispatlanmasıdır. Bu ispatı yapabilmek için düğümler çok yüksek sayıda deneme yaparlar ve bu denemeler yüksek işlemci gücü ve enerji tüketimine neden olur.

Özetleme fonksiyonları önceki bölümlerde belirtildiği üzere tek yönlü fonksiyonlardır ve belirli özet değerlerini üretebilecek girdileri elde etmek için deneme yanılmadan başka yöntem yoktur. Blockchain sistemlerinde bulmacalar genellikle blok başlığının özet değerinin belli bir değerden küçük olmasına karşılık gelmektedir. Madenciler oluşturdukları bloğun başlığının özet değerinin hedeflenen değerden daha küçük olması için yüzbinlerce bazen milyarlarca dene yapmak zorun kalırlar. Bu denemeleri yaparken madenciler blok başlığında bulunan ve rastgele bir sayıya karşılık gelen "nonce" değeri üzerinden ufak değişiklikler yaparak başlığın özet değerini yeniden hesaplarlar. Uygun bir nonce bulan madenci değer ile birlikte bloğu diğer madencilere gönderir. Diğer madenciler tek bir nonce ile hash hesaplayarak çözülen bulmacanın kolayca doğrulamasını yapmış olurlar. Çözümün doğruluğu diğer madenciler tarafından onaylandıktan sonra çözümü bulan madenci sistem tarafından ödüllendirilir. Bulmacanın sahip olduğu zorluk seviyesi hedeflenen bu hash değerine bağlıdır. Farklı blokchain sistemlerinde farklı zorluk düzeylerinde hash değerleri istenmektedir. Katılımcı sayısı ve madenci cihazlarının işlemci gücü blockchain sistemindeki bulmaca zorluğunun seviyesini etkileyen faktörlerdendir. Örnek olarak Bitcoin sisteminde her iki haftada zorluk düzeyi değiştirilerek her yeni blok oluşumunun 10 dakika civarından sabit kalması sağlanmaktadır. Zorluk seviyeleri arttıkça madencilerin tükettikleri enerji ve işlemci güçleri de artmaktadır. Bitcoin sisteminin günlük elektrik tüketimi bazı ülkelerin tüketiminden daha fazladır. Sistemin sahip olduğu bu özellik en büyük dezavantajlarından bir tanesidir.

Gerçek hayattaki değerli taşların bulunması gibi rastgele bir değerin bulunmasıyla kazanılan ödül bu işlemi yapan katılımcılara madenci adının verilmesinin sebebidir. Rastgele arama işlemine de kazma işlemi denilmektedir.

Örnek bir hash bulmacasını ele aldığımızda düğümlerin amacının "000000" ile başlayan hashler üretmek olduğunu düşünelim[9]:
SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
(çözülmedi)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10(çözülmedi)
…
SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587(çözüldü)

Bu değerin elde edile bilmesi için ilgili madencinin 10730896 deneme yaptığını görmekteyiz. Zorluk derecesini arttırmak için amaç bir sıfır eklenerek daha da zorlaştırıldığında deneme sayısının 934224175'e çıktığı görülmüştür.

Bu zorluğu azaltmak için bazı madenciler birlikte çalışarak ödüllerden birlikte faydalanma yöntemine başvurabilirler. Deneme yapılacak aralıkları aralarında paylaştıran madenciler grubun sayısı ile orantılı şekilde sonuca daha hızlı şekilde ulaşırlar. Bu yöntemde madenciler her kazanılan ödülü paylaşmak durumundadır.

3.1.2 Varlık ispatı(proof of stake) uzlaşma yöntemi

Bu yöntemin kullanıldığı blockchain sistemlerinde blok yaratma koşulu katılımcıların sisteme girerken kripto para olarak satın aldıkları ve riske ettikleri hisselere bağlıdır. Madenciler ağa dahil olurken belirli bir süre harcanamayacak şekilde istedikleri kadar kripto parayı riske ederek hisse satın alırlar. Bu satın alma bazen özel bir işlem ile veya özel bir hesaba paranın aktarılması şeklinde olur. Yatırım yapan madencilerin yeni blok yaratma olasılıkları genellikle yaptıkları yatırımın blockchain ağı genelindeki toplam yatırım miktarına oranına eşittir. Daha fazla yatırım yapan madenciler sonraki blokların üretilmesi için daha fazla şansa sahip olurlar. Yatırdığı miktar tüm hisselerin %23'ü olan bir madencinin bir sonraki bloğu yaratma ihtimali %23'e eşittir. Aynı şekilde %2'lik yatırım yapmış bir madenci bir sonraki bloğu yaratmak için %2'lik bir şansa sahiptir. Genel mantık olarak katılımcıların yaptıkları yatırımın temel faktör olduğu bu uzlaşma yöntemi pratikte uygulanırken kendi içinde çeşitli farklılıklar göstermektedir.

Bu yöntemin bir diğer kullanım şekli çoklu oylama sistemidir. Çoklu oylama sistemindeki blockchain ağlarında sistem yatırım yapmış madenciler arasından bir kısmını sonraki blok için aday olarak gösterir. Adaylar kendi aralarında birden fazla şekilde tekrar tekrar oy verirler. En çok oyu alan madenci bir sonraki bloğu üretmek

için hak kazanmış olur. Böylece her yeni blok seçiminde diğer madencilerin de söz hakkı olmuş olur.

Bir diğer metot ise madenciler tarafından yatırılan kripto paralara bir süre kısıdının konmasıdır. Sisteme giren madencinin yaptığı yatırım belirli bir zaman geçtikten sonra aktif olup madenciye blok yaratma hakkı kazandırır. Yaratılan blok sonrası madenci yine aynı süre kadar beklemek durumundadır. Böylece sistemi fazla yatırım yaparak domine etmek isteyen madenciler için de bir çözüm yöntemi sağlanmış olur.

Proof of stake yöntemi farklı kullanış biçimlerine sahip olsa da rastgele sayı denemeleri ile zorlu bulmacaların çözümüne gerek olmadığı için yüksek işlemci gücü gerektirmez ve gereksiz elektrik tüketimine yol açmaz. İşin ispatı yöntemini kullanan blockchain sistemlerinin neden olduğu gereksiz kaynak tüketimi hissenin ispatı yönteminin gelecekte daha fazla tercih edilme sebebi olabilir.

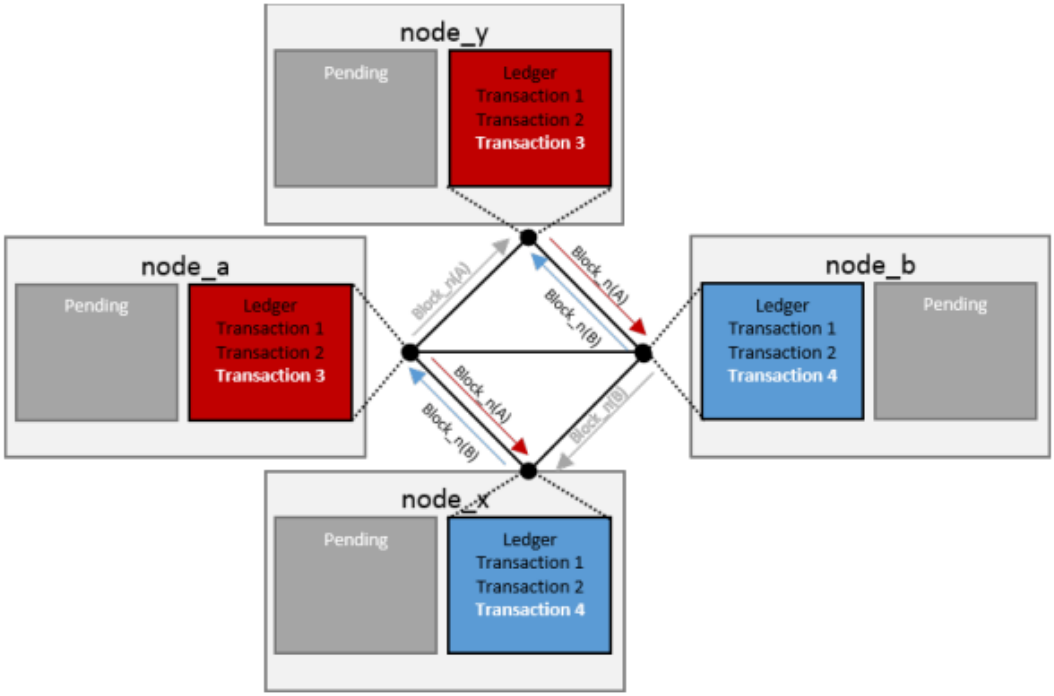
3.1.3 Round Robin uzlaşma yöntemi

Round Robin yöntemi daha çok özel blockchain sistemlerinde kullanılmaktadır. Tüm katılımcıların birbirini tanıdığı ve güvendiği bu sistemlerde sonraki bloğun kim tarafından eklendiği çok mühim değildir. Sisteme dâhil olan aktif düğümler arasında sırasıyla blok oluşturma hakkı sistem tarafından verilir. Kriptografik bulmacaların olmaması sebebiyle bu yöntemde yüksek elektrik tüketimi veya işlemci gücüne gerek yoktur. Düğümlerin birbirlerini tanıması ve güvenmesi zorunluluğu yöntemin halka açık blockchain sistemlerinde kullanılmasını imkânsız hale getirmektedir. Halka açık blokcchainlerde bu yöntem uygulansaydı sistemi ele geçirmek isteyen saldırganlar çok sayıda düğüm ekleyerek ağı kendi istekleri doğrultusunda yönetebilirlerdi.

3.2 Çakışma Ve Çözüm Yöntemleri

Blockchain ağları dağıtık sistemler oldukları için blok yaratma işlemleri katılımcılar tarafından halledilmektedir. Her ne kadar uzlaşma yöntemleri kullanılsa da aynı anda farklı düğümler tarafından farklı bloklar yaratılabilir. Bu tarz durumlar meydana geldiğinde bu karışıklığın olabildiğince hızlı şekilde çözülmesi gerekir. Çünkü farklı düğümler tarafından yaratılmış farklı bloklardaki işlem listesi aynı olmayacaktır. Her iki düğüm kendi ekledikleri blokları kayıt defterlerine ekleyip diğer düğümlere gönderecekleri için ağ genelinde birbirinde farklı iki kayıt defteri ortaya çıkacaktır. Birinde olan işlemler diğerinde olmadığı için aslında harcanmış olan kripto paralar

harcanmamış olarak görülebilir. Şekil 3.1'de node_a ve node_b düğümleri tarafından aynı anda iki farklı bloğun yaratılması durumunda kayıt defterlerindeki durum gösterilmiştir. İşlem 3 iki düğümün kayıt defterinde yer alırken diğer iki düğümün kayıt defterinde yer almaz. Aynı durum işlem 4 için ters düğümlerde geçerlidir.



Şekil 3.1: Blockchain çakışma akışı[10].

Bu tarz çakışma durumların çözümünde blockchain sistemleri bir sonraki bloğun yaratılmasını bekler. Bir sonraki bloğu yaratan kullanıcının sahip olduğu zincir versiyonu doğru olarak kabul edilir ve blokchain sisteminin devamlılığı bu versiyon üzerinden sağlanır. Diğer versiyondaki işlemler ise kullanılmamış işlem havuzuna yeniden gönderilir. Böylece karmaşıklıktan doğan iki versiyonlu blokchain sisteminde kayıt defterleri tek versiyona düşürülmüş olur.

3.3 Blockchain Çatallaşma

Tüm bilişim sistemlerinde olduğu gibi blockchain sistemlerinde de çeşitli güncellemeler gerekmektedir. Bu güncellemeler sistemde kullanılan kriptografik teknolojilerin güncellemesi olabileceği gibi ağda kullanılan yazılım operasyonlarının güncellemeleri de olabilir. Yeni blok yaratma yönteminin farklı bir algoritmayla yapılması veya uzlaşma yönteminin değiştirilmesi bu güncellemelere örnek olarak

verilebilir. Merkezi sistemlerde bile bu tarz güncellemeler zor operasyonlar gerektirirken blockchain gibi dağıtık sistemlerde bu güncellemeleri yapmak çok daha zordur. Merkezi bir sistem olmadığı için yapılan değişikliklerin sistem geneline yayılması ve katılımcıların yeni yapıya adapte olması bu zorlukların başında gelir.

Blockchain sistemlerinde yapılan güncellemelerin bazıları daha köklü değişiklikler gerektirirken bazıları daha basit değişiklikler içerir. Köklü olan güncellemelerde zincir güncel durumunda ikiye ayrılır ve kullanıcılar yeni zincire geçerek güncellemeye adapte olması konusunda zorlanır. Basit olan değişikliklerde ise katılımcıların çoğunluğunun yeni yapıya geçmesi yeterlidir tüm kullanıcılar güncellemeye adapte olması konusunda zorlanmazlar. Basit veya daha karmaşık olan bu güncellemelerle birlikte blockchain zincirinde meydana gelen ayrışmalara çatallaşma adı verilir. Çatallaşmalar basit ve zorunlu çatallaşma olarak iki ayrı başlık altında incelebilir.

3.3.1 Basit çatallaşma

Bu ayrışma tipinde kullanıcılar güncelleşmeyi alma konusunda zorlanmazlar. Yeni eklenen değişiklik uygulanmasa da madenciler hayatlarına devam edebilirler. Genellikle basit yazılımsal değişiklikler bu kategoriye girer. Blok doğrulama aşamasında kullanılan metotların yeni versiyonlarının sisteme eklenmesi örnek olarak gösterilebilir.

3.3.2 Zorunlu çatallaşma

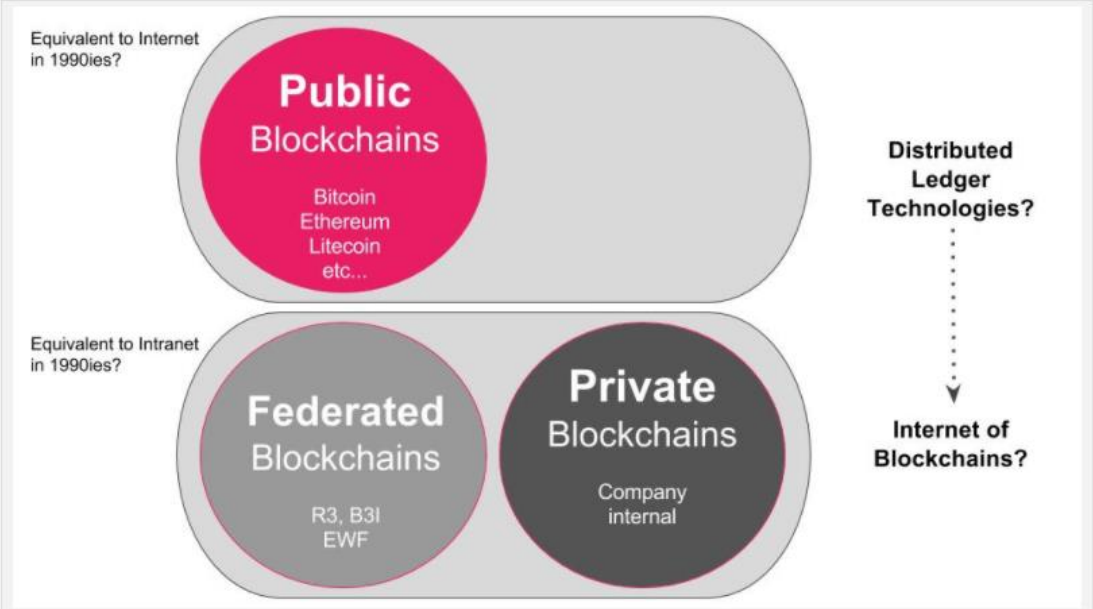
Zorunlu ayrışmalara blockchain sistemini kökten değiştiren güncellemeler sebep olur. Katılımcılar güncellemeleri almak konusunda zorlanırlar. Güncellemeyi almayan madenciler sistemde kalmaya devam edemezler. Bu tarz güncellemeler genellikle kullanılan kriptografik fonksiyonların değişikliklerini içerir. Blok başlıklarının hash'inin alınmasında kullanılan fonksiyonlarda meydana gelecek bir değişiklik yeni blokların doğrulanmasında kullanılacağı için tüm madenciler bu güncellemeyi almak zorundadırlar. İşlemlerin imzalanmasında kullanılan asimetrik algoritmanın değişmesi bir diğer örnek olarak verilebilir. İmzalama yönteminde yapılacak bir güncellemenin tüm madenciler tarafından alınması mecburidir. Eğer bu güncelleme alınmazsa işlemlerin doğrulanması yapılamaz. Bu ayrışma meydana gelirken sistemde var olan güncel haliyle tüm kullanıcılar ve onlara ait kripto paralar yeni versiyona aktarılır. Madenciler ve kullanıcılar yeni zincir üzerinden işlemlerine ve doğrulamalarına devam ederler. Bazı blockchain sistemlerin bu çatallaşmalar sonrası yeni kola farklı

bir isim verilerek iki yapının da çalışması sağlanır. Bitcoin yıllar içerisinde ayrışmalara giderek Bitcoin Cash ve Bitcoin Gold gibi yeni kollara ayrılmıştır.

3.4 Blockchain Çeşitleri

Blockchain sistemlerinde teknolojide kullanılan farklı özellikler baz alınarak çeşitli sınıflandırmalar yapılabilir. Bitcoin projesinin başarısı ve geniş kitlelere yayılması blockchain teknolojisine olan güveni artırmakla birlikte blockchain teknolojisinin farklı sektörlerde farklı süreçler için de kullanılabileceği fikrini doğurmuştur. Blockchain teknolojisi herhangi bir değerin transferi için kullanılabileceği gibi kişiler arası sigortacılık, enerji ticareti, araç kiralama benzeri işlemlerin sözleşmelerinin yapılması ve paylaşılması için de kullanılabilir. Bazı firmalar bu tarz projeleri geliştirirken doğrudan bitcoin blockchain protokolünü kullanırken bazı firmalar ise değişen ihtiyaçlar doğrultusunda farklı blockchain protokolleri geliştirmiştir. Etherum blockchain protokolü bunlardan bir tanesidir ve blockchain ağında mantıksal programlama yapmaya olanak sağlaması açısından devrim niteliğindedir[11]. Bu mantıksal programcıklara akıllı sözleşmeler adı verilir ve kullanılan farklı protokollere göre de blockchain sistemlerinde sınıflandırma yapılabilir.

Bir diğer sınıflandırma ise blockchain ağına katılımın izne tabi olup olmaması ile ilgilidir. Bitcoin gibi bazı ağlarda blockchain sistemi herkese açıktır ve isteyen katılabilir. İzne tabi olan ağlar ise özel ağlardır ve katılmak için yetkili bir merciden izin almak gerekir. İzne tabi olan özel blockchain ağlarının ortaya çıkışı birbirini tanıyan kurumların bir araya gelerek çalışma birlikleri kurmasıyla olmuştur. Bu şirket ve kurumları böyle bir yapıya yönelten fikir blockchain teknolojisinin bel kemiği olan ortak kayıt defteridir. Şekil 3.2'de katılım izni açısından yapılan sınıflandırma görülmektedir. Özel blockchain ağları şirket içi ağlar olarak düşünülebilir ve klasik bilişim sistemlerindeki intranet ağlara karşılık gelmektedir. Blockchain teknolojisinin temel özellikleri düşünüldüğünde bu tipin kullanım alanları oldukça kısıtlıdır. Özel ağlardan herkese açık olan ağlara doğru gittikçe dağıtıklık oranı artmaktadır.



Şekil 3.2: Blockchain tipleri[12].

3.4.1 Herkese açık blockchain sistemleri

Bu tip blockchain ağlarına katılım için herhangi bir otoriteden yetki almak gerekmez. Dünya üzerinde herhangi birisi ilgili blockchain protokolünün yazılımını indirerek kendi cihazları üzerinde bir düğüm kurabilir ve madenci olabilir. Katılım için izin gerekmeyen bu ağlarda madenciler işlemler yaratabilir, var olan işlemleri izleyebilir ve işlemleri doğrulayabilirler. Bu tip ağlarda işlemler transparan şekilde izlenebilirken aynı zamanda anonimlik de korunmaktadır. Bu tarz blockchain sistemlerine Bitcoin, Etherum, LiteCoin, Monero gibi ağlar örnek olarak verilebilir. Hangi hesaptan hangi hesaba ne kadar tutarda gönderim yapıldığı herkes tarafından görülebilirken bu hesapların kime ait olduğu sahipleri tarafından bilinmektedir.

Herkese açık blockchain sistemleri sahip olduğu özellikler sayesinde dağıtık uygulama mimarilerin kullanıldığı yazılım ve bilişim sistemleri için büyük kolaylıklar sağlamaktadır. Dağıtık mimaride uygulama geliştirmek isteyenler var olan bu ağlardan faydalanarak maliyetleri düşürebilmektedirler böylece sunucu ve donanım gibi masraflar bir ölçüde azaltılmış olur.

3.4.2 Birlik blockchain sistemleri

Bu tip blockchain sistemlerinde blockchain ağına katılım herkese açık değildir. Ağa katılmak ve işlem doğrulamak için onay merciinden izin almak gerekir. Genellikle

belli amaçlar doğrultusundan bir araya gelerek birlikler oluşturmuş kurumlar ve şirketler arasında kurulan blockchain ağlarıdır. Ağın yönetimi bu şirketlerin temsilcilerinden oluşan bir grup tarafından yapılmaktadır. Ağa dâhil olmak için kurulmuş olan bu birliğin üyesi olunması ve sözleşmelerin yapılmış olması gerekir. Bu tip sistemlerde işlemleri hangi düğümlerin doğrulayacağı hangilerinin kontrol edeceği gibi konular yine ortak kararlar alınarak verilmektedir. Sistemler dışarıya kapalı ve birbirlerini resmi olarak tanıyan kurumlar arasında olduğu için işin ispatı gibi yüksek kaynak gerektiren uzlaşma yöntemleri kullanılmamaktadır. Bu sebeple bu tarz sistemlerde işlemlerin bloklar haline getirilmesi ve doğrulanması çok daha hızlı şekilde gerçekleştirilir. Aynı zamanda enerji sarfiyatı ve gerek duyulan işlemci gücü de çok daha azdır.

Günümüzde genellikle finans sektöründeki firmaların oluşturduğu birlikler bulunmakla beraber dünyanın çeşitli ülkelerinden farklı firmaları bir araya getiren sigortacılık, sağlık ve enerji sektörüne odaklanmış birlikler de vardır. Finans sektörü için en bilinen örneklerin başında R3 organizasyonu gelmektedir. R3 firması liderliğinde olan bu birliğe 100'ü aşkın banka, finans kuruluşları, profesyonel teknoloji firmaları, ticari kurumlar dâhildir ve birlik üyeleri kendi dağıtık kayıt defteri teknolojisi olan Corda platformunu geliştirmektedir[13]. Açık kaynak olan bu platforma birlik üyeleri katkı yapmakta ve iş hayatının ihtiyaçlarına uygun bir platform sunmayı amaçlamaktadırlar. Bu organizasyon 2015 yılında dağıtık sistemlerin sahip olduğu özellikleri iş dünyasına taşıma amacıyla kurulmuştur.

3.4.3 Özel blockchain sistemleri

Kurum veya şirketlerin kendi içlerinde özel kurulmuş blockchain sistemleridir. Bu tip sistemlerde kimlerin blockchain ağına katılacağı ve kimlerin madencilik yaparak yeni blokları oluşturabileceği ağa sahip olan şirket tarafından yönetilmektedir. Yeni işlem oluşturma izne tabi olurken blockchain ağındaki işlemlerin okuma yetkisi herkese açık olabilir bu tamamen sahip olan otoritenin yönetimindedir. Çıkış noktası dağıtık olmak üzerine olan bir teknolojinin bir şirket içerisinde özel olarak kullanılması blockchain teknolojisinin ruhuna çok uygun olmasa da teknolojinin diğer özelliklerinden faydalanmak için şirket içi çözümlerde bu tip blockchain yapıları kullanılmaktadır.

3.5 Blockchain Kullanım Senaryoları

Blockchain teknolojisi ortaya çıkış tipi ve barındırdığı potansiyel sebebiyle birçok uzman tarafından internet teknolojisine benzetilmektedir. İnternetin hayatımıza girdiği 90'lı yıllardan bugüne kadar günlük yaşamda ve iş hayatında internet ile birlikte çok büyük değişimler yaşanmıştır. Bu değişimlerin bir benzerinin blockchain teknolojisi ile de olacağı öngörülmektedir. Blockchain teknolojisi sağladığı özelliklerle günümüzde var olan birçok sektörü ve sektörlerdeki iş yapış şekillerini kökünden değiştirmeye aday olarak öngörülmektedir. Finansal servisler maliyetleri düşürmesi açısından blockchain teknolojisinin sağladığı imkânları ilk fark eden sektör olmuştur fakat blockchain teknolojisi sağlık, sanayi, eğitim, enerji, lojistik ve tedarik zinciri gibi birçok iş alanında kullanım potansiyeline sahiptir[14]. Güncel olan her konuda olduğu gibi blockchain konusunda da toplumun ve iş dünyasının ilgisi üst düzeydedir fakat bu ilgi zaman zaman yanlış yönlendirmelere ve popüler söylemlere sebep olmaktadır. Unutulmaması gereken nokta bu teknolojinin sihirli bir değnek olmadığıdır. Teknolojinin özellikleri tam incelenmeden temel felsefesi anlaşılmadan yapılacak girişimler büyük oranda başarısızlıkla sonuçlanabilir. Uzmanların, mühendislerin, sektörlere yön veren yöneticilerin üzerine düşen en önemli görev araştırma geliştirmeye vakit ve bütçe ayırarak teknoloji konusunda derin bir bilgi birikime sahip olunmasıdır. Ancak bu bilgi ve birikim ışığında sektörlerdeki güncel iş yapış şekilleri analiz edilerek uygun görülenler üzerinden blockchain dönüşüp projeleri başlatılabilir. Bir diğer dikkat edilmesi gereken nokta teknolojinin yeni olması sebebiyle riskler barındırmasıdır. Üretim ortamlarında çalışacak projelerden önce şirketler ve girişimciler konsept doğrulama çalışmaları yaparak bu riskleri en aza indirebilirler. Gartner blockchain raporunda verilen bilgiye göre blockchain teknoljisine erken adapte olanlar için 5-7 yıl arasında bir risk dönemi bulunmaktadır[14].

Blockchain'in sahip olduğu temel özellikler ve sağladığı faydalar kullanılabilecek sektörleri öngörme konusunda yardımcı olabilir. Temel özellikleri ve faydaları olarak aşağıdakiler sayılabilir;

- Aracı 3.kişilere ihtiyaç olmaması
- Düşük işlem maliyetleri
- Geliştirilmiş nakit akışı
- İşlemlerin geçmişe yönelik değiştirilememesi
- Transparanlık ve işlemlerin takibi

- İşlemlerin hızlı gerçekleşmesi
- Kriptografik güven
- Gerçek dijital varlık ve sahiplik kavramı

Blockchain teknolojisi üzerine Gartner raporunda yer alan analiz şekil 3.3'te gösterilmiştir.

Güçlü Yönler	**Zayıf Yönler**
• Dağıtık esneklik ve kontrol • Merkezi olmayan ağ • Açık kaynak • Güvenlik ve kriptografi • Varlık ispatı • Yerel varlık yaratma • Dinamik ve akıcı değiş tokuş	• Kayıt defteri birlikte çalışabilirliğindeki eksiklikler • Zayıf kullanıcı deneyimi • Test edilmiş teknoloji eksikliği • Geliştirici araçlarındaki eksiklikler • Cüzdan ve anahtar yönetimi • Yetenek azlığı ve maliyetleri • Yeni teknoloji sağlayıcılarına olan güven eksikliği
Fırsatlar	**Tehditler**
• Düşük işlem maliyetleri • İş süreçlerinde hızlanma ve efektiflik • Dolandırıcılık işlemlerinde azalma • Sistemsel risklerde azalma • Parasal demokratikleşme • Yeni iş modelleri • Uygulamaların rasyonelleştirilmesi	Yasal sınırlamalar Siyasi aktörler Teknoloji hataları Kurumsal entegrasyon sınırları Farklı blockchain sistemleri Kayıt defteri çakışmaları Yönetim eksikliği

Şekil 3.3: Blockchain swat analizi

3.5.1 Bankacılık

Blockchain teknolojisini hayata geçiren ilk projenin para transferine olanak sağlayan finansal bir uygulama olması bankacılık sektörünü bu teknolojide önemli bir potansiyel alanına dönüştürmektedir. Günümüzde bankalar kendi içlerinde merkezi bilişim sistemleri ile teknoloji ve yazılım ihtiyaçlarını gidermektedir. Bankalar parasal tüm işlemleri kendi ağ cihazları, sunucuları, yazılımları ve veritabanları üzerinden gerçekleştirir. Diğer bankalarla veya merkez bankası gibi regülasyon kurumlarıyla olan iletişimler entegrasyon servisleri aracılığıyla olmaktadır. Güvenilir kurum ihtiyacı ve aracı bankalarla olan entegrasyonlar bankacılık işlemlerinde hem süreleri hem de masrafları arttırmaktadır. Blockchain teknolojisi sahip olduğu temel özellikler sebebiyle bankacılık sektörünün bu problemlerini ve süreçlerini kökünden

değiştirmeye aday bir teknoloji olarak görülmektedir. Teknolojinin sahip olduğu potansiyeli fark eden sektör temsilcileri bu alana hızla yatırım yapmakta ve olası senaryolarını merkezi sistemlerden dağıtık sistemlere taşımaya çalışmaktadırlar. Yeni gelişen bir teknoloji olması sebebiyle yapılan çalışmalar titizlikle ve temkinli bir şekilde yürütülmektedir. Blockchain teknolojisinin kullanılmasıyla bankacılık sektörünün masraflarının azalacağı öngörülmektedir. Financial Times'ta yeralan araştırmaya göre bu teknolojiye entegrasyonla birlikte üçüncü parti masraflarında yaklaşık 20 milyar dolar bir tasarruf olacaktır[15]. Santander Fintech tarafından hazırlanan başka bir raporda ise blockchain kullanımının 2022 yılı civarında bankaların bilişim altyapı ve donanım masraflarında 15-20 milyar dolar civarında bir tasarruf sağlayacağı tahmini yer almaktadır[16].

Accenture firması öngürülerin bir adım ötesine geçip daha somut bir analiz yapmak üzere 2017 yılında McLagan firması ile ortak bir çalışma yapmıştır. McLagan firması bu çalışma kapsamında dünyanın önde gelen yatırım bankalarının verilerini Accenture ile paylaşmıştır. 50 adet operasyonel masraf ölçütünü barındıran bu araştırmanın sonuçlarına göre dağıtık sisteme geçmenin bankalara finans raporlamaları açısında %70 civarında bir tasarruf sağlaması beklenmektedir. Ayrıca aynı rapora göre merkezi operasyon ve mutabakat masaraflarında %50 civarında bir tasarruf öngörülmektedir[17].

Blockchain teknolojisinin bankacılık sektöründeki en bilinen uygulamalarından bir tanesi olarak Ripple gösterilebilir. Ripple firması tarafında geliştirilen platform özellikle uluslararası para transferini gerçekleştirmek için kurulmuştur. Ripple kulllanan bankalar müşterilerine farklı ülkelerden ripple kullanan bankalara para transferini merkezi sistemlere göre daha ucuz ve daha hızlı şekilde sunmaktadır. Bu özelliğiyle SWIFT gibi merkezi yapıların yakın gelecekteki en büyük rakibi olarak Ripple görülebilir. Bu sistemin en büyük avantajı muhbir bankalara ve diğer aracılara ihtiyaç duymadan hızlı, izlenebilir ve düşük masraflı para transferine olanak sağlamasıdır.

Finans sektöründe blockchain konusunda öncü olan bir diğer girişim ise R3 organizasyonudur. R3 firması öncülüğünde 100'den fazla banka ve finans kuruluşuyla birlikte yürütülen çalışmalarda hedeflenen şey finansal operasyonlar için yeni bir dağıtık işletim sisteminin orataya koyulmasıdır. Bu amaç doğrultusunda Corda

platformu geliştirilmiştir. Corda ile bankaların kendi senaryolarını dağıtık sistemelere taşımaları hedeflenmektedir.

3.5.2 Sigortacılık

Bankacılık sektöründe olduğu gibi sigortacılık sektöründe de işlemler aracı kurumlar üzerinden yapılmaktadır. Blockchain teknolojisi özellikleri itibariyle sigortacılık dünyasının dijital dönüşümüne katkı sağlayacak potansiyeli barındırmaktadır. Primlerin ödenmesi, risklerin hesaplanması, geçmişe yönelik verilerin doğruluğu ve tazminatlar sektörün temel yapıları olarak sayılabilir. Blockchain teknolojisi prim ve tazminat ödemelerinde hem şeffaflığın sağlanmasında hem de akış trafiğinin takibinin yapılmasında kullanılabilir. Dolandırıcılık işlemleri sigortacılık sektörünün en büyük problemi olarak gösterilmektedir. Deloitte tarafında yapılan bir araştırmaya göre her yıl yaklaşık 400 milyon pound değerinde dolandırıcılık işlemi meydana gelmektedir. Para için kaza anlamına gelen bu dolandırıcılık tipinde dolandırıcılar gerçek kaza görüntüsü verdikleri bu senaryolar ile sigorta firmalarından tazminat talep etmektedirler. Özellikle sektör geneli ortak bir veri havuzunun bulunmaması ve müşterilerin geçmiş kayıtlarına sağlıklı şekilde ulaşılamaması büyük oranda bu dolandırıcılık faaliyetlerine imkân tanımaktadır.

Blockchain teknolojisinin kullanılmasıyla birlikte sözleşmeler ve tazminat talepleri dağıtık ve herkese açık kayıt defterlerinde tutulacaktır. Kayıt defterlerinin sektör genelindeki tüm sigortacılarda olması ve bu kayıtlara yeni işlemlerin eklenmesi uzlaşma yöntemleri ile olacağı için bir kaza için birden fazla tazminat ödenmesinin önüne geçilecektir. Sektör geneli veriler açık olacağı için risk analizleri yapılırken daha doğru sonuçların ortaya çıkması öngörülmektedir. Akıllı sözleşmelerinde kullanımıyla birlikte belirli koşulların meydana gelmesiyle sigorta tazminatlarının otomatik ödenmesi süreçleri blockchain teknolojisinin sigortacılık sektörüne bir diğer katkısı olacaktır. Ayrıca bu tazminat ödemelerinin doğrulanması da yine uzlaşma yöntemleri kullanılarak sisteme dâhil diğer sigorta şirketlerinin düğümleri tarafından yapılacaktır. Blockchain sistemlerinde verilerin geçmişe yönelik değiştirilememesi dolandırıcıların gerçek kimliklerini saklamasına engel olacaktır. Tüm bu yönleriyle blockhain uygun senaryolarda kullanıldığında sigorta sektörüne önemli derecede katkı sağlayacaktır.

3.5.3 Emlak

Dijital dünyada sahiplik kavramının gerçek anlamda uygulanabilmesi merkezi sistemlerle çeşitli zorluklar barındırmaktadır. Emlak sektörü bu zorluklar sebebiyle dijitalleşme süreçlerinde çeşitli sorunlara sahiptir. Ev ve arsa gibi taşınmazların alım-satım geçmişlerinin halka açık takip edilememesi ve kayıtların resmi kurumlarda merkezi sistemlerde tutulması bu sektörü dolandırıcılığa açık hale getirmektedir. Merkezi sistemlerde yapılacak ufak değişikliklerle veya sahte tapu belgeleriyle büyük miktarlarda dolandırıcılık işlemi gerçekleşebilir. Blockchain kullanılmasıyla birlikte sahiplik kavramı gerçek anlamda dijital dünyaya taşınmış olacaktır. Tüm alım satım işlemlerinin blockchain üzerinden yapıldığı bir senaryoda veriler dağıtık şekilde tutulacağı için geçmişe yönelik bir manipülasyon yapılamayacaktır. Ayrıca bir taşınmazın geçmiş sahipleri sorgulanmak istendiğinde doğruluğuna emin bir şekilde veriler elde edilebilir. Halka açık şekilde işlemlerin takip edildiği böyle bir sistemde dolandırıcılık olayları en aza indirilecektir. Ayrıca alım-satım işlemlerinin blockchain üzerinden yapılması güvenilir üçüncü şahıs ihtiyacını ortadan kaldıracağı için sektör geneli masraflar azalacaktır. Velox firması tarafından hayata geçirilen blockchain tabanlı proje ile tüm bu hedefler ABD Chicago'da uygulanmak istenmektedir. Pilot aşamasında olan bu proje emlak sektörünün dijitalleşmesine önemli katkılar yapmaya adaydır.

3.5.4 Enerji ticareti

Enerji sektöründeki ticarette aracı operasyonları hem yüksek maliyetlere hem de zaman kaybına sebep olmaktadır. Alım satım yapan şirketler arası fiyat belirleme ve belirlenen fiyatlar üzerinden yapılacak satın almalar için çok miktarda belge hazırlanmakta ve bunlar çeşitli yasalara göre raporlanmaktadır. Tüm bu operasyonlar aracı şirketler ve piyasayı belirleyen borsacılar tarafından yürütülmektedir ve bu operasyonlar merkezi bilişim sistemleri tarafından yönetilmektedir. Verinin güvenliği ve bütünlüğü birden fazla aktörün olduğu bu tarz sektörlerde her zaman için potansiyel sorunlar arasındadır. Ayrıca doğru olan veriye hızlı ulaşma ve güncel durum hakkında kolayca bilgi sahibi olma şirketlerin ve müşterilerin birinci önceliklerindendir. Blockchainin bu sektörde kullanılmasıyla hem fiziksel enerjinin takip edilebilirliği artarken hem de operasyon maliyetleri azalarak birim maliyetleri düşmesine yardımcı olacaktır.

Enerji ticareti eski dönemlerde sadece şirketler arasında olsa da özellikle güneş enerjisinden elektrik üretiminin artmasından sonra bu ticaret kişiler arasına kadar inmiştir. Ev sahipleri ürettikleri fazla miktarda enerjiyi çeşitli platformlar aracılığıyla satma ihtiyacı duymaktadır. Enerji sektörünün sahip olduğu klasik yapı bu ihtiyaca cevap vermeye yeterli değildir. Bu alandaki sıkıntıyı çözmek üzere yola koyulan bazı girişimciler blockchain teknolojisini kullanarak aracıları devre dışı bırakan bir enerji ticaret platformu kurmuşlardır. Evlerin ne kadar üretim yaptığı ne kadar ödemenin gerçekleştiği ne kadar satımın yapıldığı gibi tüm bilgiler platform üzerinden takip edilebilmektedir. Tüm bilgiler blockchain ağında dağıtık bir şekilde tutulmaktadır. Bu da katılımcılar arası güveni oluşturmaktadır.

3.5.5 Sağlık

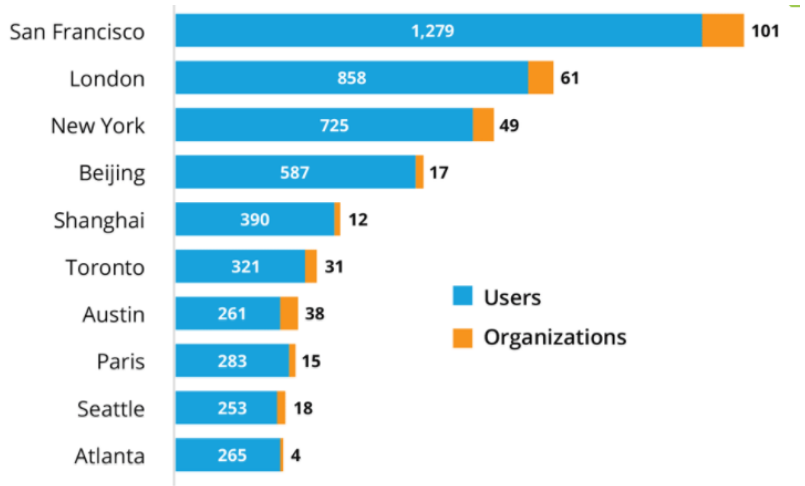
Sağlık sektörü dijital süreçlerin yoğunlukla kullanıldığı başlıca alanlardandır. Birden fazla aktörün yer aldığı bu sektörde hastaneler, ilaç sağlayıcıları, doktorlar, eczacılar ve hastalar gibi birçok aktör arasında çeşitli dijital süreçler işletilir. Tüm bu süreçler çok yüksek sayıda işlemin oluşmasına ve büyük miktarda verinin ortaya çıkmasına sebep olur. Bu denli kritik ve büyük bir sektörde ortaya çıkan bu verilerin güvenliği ve istenildiğinde doğru bilginin kolayca elde edilmesi çok önemlidir. Bir hastanın tahlil sonuçları veya kullandığı bir ilaç bu veriler arasında sayılabilir. Sağlık verileri kişisel gizli bilgi olarak değerlendirildiği için sadece ilgili kişilerce paylaşılması çok önemlidir. Günümüzde merkezi sistemlerle yönetilen sağlık sektörü için bazı blockchain girişimleri oldukça iddialı alternatif çözümler sunmaktadır. Verinin gerçek sahipliği kavramından yola çıkan bu girişimler hastaya sağlık bilgilerinin kiminle paylaşılacağının onayını almadan herhangi bir paylaşıma izin vermemektedir. Ayrıca verilerin hash değerleri blockchainler üzerinde dağıtık olarak tutulduğu için verilerin geçmişe yönelik manipüle edilip edilmediği kolayca anlaşılmaktadır. Ayrıca farklı hastaneler ve ilaç sağlayıcıları arasındaki ayrı ayrı entegrasyon ihtiyaçları ortadan kaldırılarak tek bir blockchain platformu üzerinden tüm süreçlerin işletilmesi mümkündür.

3.6 Dağıtık Uygulamalar

Blockchain teknolojisinin gelişmesiyle birlikte dağıtık uygulama kavramı yazılım geliştirme terimlerinin arasına girmiştir. Günümüzdeki merkezi uygulama

mimarilerinde yazılım geliştiriciler kaynak kodlarını derleyerek merkezi sunucular üzerinden yayına açarak insanlara hizmet vermektedirler. Uygulamanın mantıksal işler yapan ve akışları barındıran kod parçaları bu merkezi sunucular üzerinde tutulmaktadır. Dağıtık uygulamalar mimarisi merkezi mimariden çok farklıdır. Dağıtık uygulamaların iş yapan mantıksal kod parçaları blockchain üzerinde yer alır ve bu programların çıktıları yine blockchain üzerindeki kayıt defterlerinde dağıtık şekilde tutulur. Dağıtık uygulamaların html, css, js gibi önyüzleri merkezi sistemlerde barındırılabileceği gibi dağıtık sunucu hizmetleri üzerinde de servis edilebilir. Bir uygulamanın dağıtık uygulama olabilmesi için iş yapan programların blockchain üzerinde barındırılması ve çıktıların yine blockchain kayıt defterlerinde saklanması gerekir. Ayrıca dağıtık uygulamalar bitcoin ve etherum gibi token bazlı bir yapı üzerine kurulmalıdır. Blockchainler üzerinde dağıtık uygulama geliştirmeye olanak veren etherum, hyperledger, ripple gibi farklı platformlar bulunmaktadır. Dağıtık uygulamaların doğası gereği genellikle projeler açık kaynaklı olarak yürütülür. Böyle yeni bir teknolojide uygulama geliştiriciler için diğer yazılımcıların katkıları ve fikirleri çok büyük öneme sahiptir.

Dünya genelinde dağıtık uygulama geliştirmeye yönelik son yıllarda artan bir eğilim mevcut. 2017 yılında Deloitte firması tarafından GitHub platformu üzerinde yapılan bir araştırmada dünya genelinde toplam 87 bin civarında blockchainler üzerinde çalışan dağıtık uygulamanın olduğu söylenmektedir[18]. Her yıl ortalama 25 bin yeni proje bu ekosisteme dâhil olmaktadır. Yapılan blockchain projelerinin coğrafi dağılımı incelendiğinde özellikle ABD ve uzak doğu ülkeleri öne çıkmaktadır. Şekil 3.4'te şehirlere göre blockchain uygulaması sayıları incelenmiştir.



Şekil 3.4: Şehirlere göre dağıtık uygulama sayıları

Türkiye geneli için rakam 97 iken bu projelerin 44 tanesi İstanbul iline aittir. Yazılım geliştiriciler için yeni bir alan olan dağıtık uygulama geliştirme süreçlerinde farklı yazılım dilleri kullanılabilmektedir. Çeşitli kütüphaneler aracılığıyla yazılımcılar aşina oldukları ve bildikleri diller ile dağıtık uygulama geliştirme imkânına sahiptir. Aynı araştırmada yer alan verilere göre dağıtık yazılım geliştirilirken en çok kullanılan dil JavaScript'tir. JavaScriptin ardından en çok kullanılan diller listesinde Pyhton, C++ ve Go gelmektedir. Go Etherum blockchain sisteminin protokol düzeyinde geliştirildiği yazılım dilidir. Bu listede yer alma sebebi Etherum platformunun açık kaynak kodlu olarak GitHub üzerinde yayında olmasıdır. Finansal sistemler geliştirilirken genellikle C++ performans ve güvenlik çekinceleriyle tercih edilmektedir. Bu tercih kendisini dağıtık uygulamalarda da göstermiştir. Blockchain – finans ilişkisi projelerde kullanılan yazılım dili istatistiklerini de bu yönde etkilemiştir.

GitHub üzerindeki blockchain uygulamalarının %90'lık kesimi kullanıcılar tarafından geliştirilirken %10'luk bir kısmı şirketler tarafından geliştirilmektedir. Araştırmada yer alan verilere göre var olan projelerin ortalama aktif kalma süreleri 1 yıldır ve arkasında şirketlerin olduğu blockchain uygulamalarının daha kalıcı olduğu görülmektedir. Şirketler tarafından geliştiriciliği yürütülen projeler daha kapsamlı olmakla birlikte proje çıktıları diğer yazılım geliştiricilere dağıtık uygulama geliştirmeye imkân tanıyan platformlar haline gelebilmektedir. Bitcoin, etherum, ripple, corda gibi platformlar githubda yer alan bu tip projelere örnek olarak gösterilebilir. Yazılım geliştiriciler bu platformları kullanarak kendi test ağlarını kurup bu ağlarda çeşitli akıllı sözleşmeler devreye alabilirler. Akıllı sözleşme geliştirip derlemeye imkân sağlayan bu platformlar uçtan uca dağıtık bir uygulamanın sahip olması gereken özellikleri yazılım geliştiricilere sunmaktadır. Etherum platformu üzerinde geliştirilmiş 1367 dağıtık uygulama bulunmaktadır[19].

4. ELEKTRONİK SAĞLIK VE GÜVENLİK PROBLEMLERİ

4.1 Elektronik Sağlık Tanımı

Tıp bilimi yüz yıllardır önemli bilim alanları arasında gösterilir. İnsanlığın ilk zamanlarından günümüze sağlık insanların birinci önceliği olmuştur. Dünyanın çeşitli ülkelerinde her yıl milyonlarca insan tedavi görmekte ve şifa bulmaktadır. Gelişen teknolojiyle birlikte tedavi yöntemleri de gelişmekte ve bu gelişmeler tıp bilimine katkı sağlamaktadır. Özellikle bilgi ve iletişim teknolojilerinin son yıllarda sağlık sektöründe kullanılması bu sektöre büyük katkılar sağlamıştır. Bilgisayarların ve mobil cihazların kullanılmasıyla birlikte e-sağlık denilen yeni bir kavram hayatımıza girmiştir. Dijitalleşen her sektörde olduğu gibi sağlık sektöründe de dijitalleşmeyle birlikte çeşitli problemler meydana gelmiştir. Güvenlik ve gizlilik bu problemlerin en başında gelir.

Dünya Sağlık Örgütü tarafından yapılan tanıma göre sağlık için bilgi ve iletişim teknolojilerinin kullanılmasına e-sağlık denir[20]. Birden fazla kurum tarafından yapılmış olan farklı e-sağlık tanımları olsa da tüm tanımların üzerinden durduğu nokta sağlık için bilgisayar, internet ve akıllı telefonların kullanılmasıdır.

4.2 E-Sağlık Bileşenleri

E-Sağlık kavramı tıp alanında birçok alt başlığı içermektedir. Elektronik sağlık kaydından tele sağlık hizmetlerine kadar birçok alan e-sağlık kavramının alt başlığı olarak düşünülebilir.

- Elektronik sağlık kaydı: Hastaların özel sağlık bilgilerini içeren elektronik kayıtlara verilen isimdir. Bu kayıtlar sağlık uzmanları tarafından tedavide ve karar vermede kullanılır.
- E-Öğrenme: Bilgi iletişim teknolojilerinin tıp eğitimi için kullanılmasına denir.
- M-Sağlık: Halk sağlığı ve medikal alanında akıllı telefonlar, saatler ve mobil nesnelerin kullanılmasıdır.

- Standardizasyon ve birlikte çalışabilirlik: Sağlık sektöründe bulunan farklı teknoloji ve yazılımların birbirleriyle olan iletişimlerinin düzgün bir şekilde olmasını sağlayan her türlü kural, yasa ve ilkeler bütünüdür
- Sağlık IT sistemleri: Sağlık sistemlerinde kullanılan ağ cihazları, sunucular, veri tabanları ve uygulamalar bütünüdür.
- Büyük Veri: Sağlık verilerinin makine öğrenmesi ve yapay zekâ yardımıyla anlamlandırılarak tanı ve tedavi süreçlerinin iyileştirilmesi

4.3 E-Sağlığın Faydaları

Elektronik sağlık alanındaki gelişmeler tıp bilimine ve uygulamalarına birçok fayda sağlamaktadır. Hastalar, doktorlar, hastaneler ve sağlık sektöründeki diğer aktörler teknolojinin bu alandaki getirilerinden faydalanmaktadırlar. Elektronik sağlıktaki gelişmelerin sağladığı yararlar şunlardır;

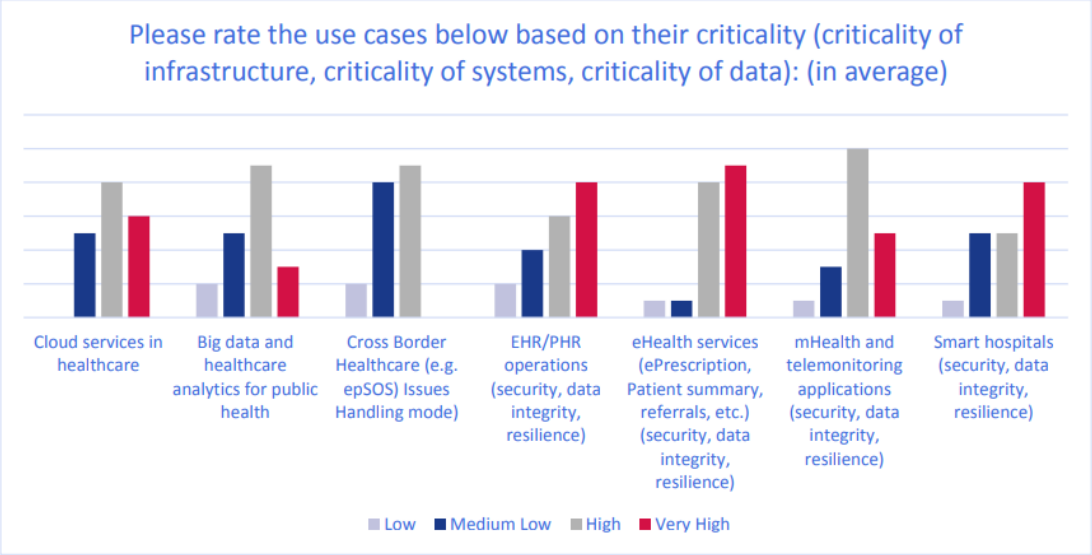
- Sağlık masraflarında önemli ölçüde azalma
- Medikal hata oranlarında düşme
- Tedavi kalitesinde yükselme
- Tıp eğitiminde ve istatistik çalışmalarında kolaylık
- Bilgilerle doğrulanmış tedavi kararlarına yardımcı
- Hasta hareketliliğinde artış

4.4 Elektronik Sağlık ve Güvenlik

Bilgi ve iletişim teknolojisini kullanan ve içerisinde bilgisayar, internet ve mobil cihazlar içeren her sektör bir takım güvenlik zafiyetleri barındırır. Bu durum bilgi teknolojilerinin doğasından gelir. İnternet erişimi olan her sistemin kontrolü ele geçirilebilir ya da kritik bilgiler çalınabilir. Konu sağlık bilgileri olduğunda bu güvenlik meselesi daha önemli bir hale gelmektedir.

ENISA tarafından Avrupa birliği üye ülkelerinde bulunan sağlık sektöründeki şirketler arasında yapılan araştırmaya göre elektronik sağlık sektöründeki güvenlik çekinceleri hayli yüksektir. Araştırma sonuçları şekil 4.1'de verilmiştir. Özellikle mobil cihaz kullanımındaki artış ve üretilen büyük miktarda elektronik sağlık verisi karmaşık güvenlik ve gizlilik sorunlarına yol açmaktadır. Bu problemlerin başlıca sebepleri olarak şunlar sıralanabilir; yetersiz yasal düzenlemeler, eksik koruma önlemleri ve

kusurlu teknik sistem mimarisi. Elektronik sağlık alanında güvenlik iki ana başlık altında incelenebilir; yasal çerçeve ve teknik güvenlik.



Şekil 4.1: E-Sağlık enisa araştırma sonuçları.

4.4.1 Yasal çerçeve

Elektronik sağlık sistemleri kullanan firmalar güvenlik, gizlilik, bütünlük ve erişilebilirlik açısından çeşitli zorluklarla karşılaşmaktadırlar. Ulusal ve uluslararası düzeyde çeşitli kurum ve organizasyonlar tarafından bu zorlukları aşma konusunda firmalara yardımcı olmak için bir takım standartlar ve ilkeler kitapçıkları yayınlanmaktadır. Firmalar yol haritası olarak bu standartları kendi kurumlarında uyguladıklarında hasta sağlık verilerinin güvenliği ve gizliliği hakkında gerekli önlemleri almış olurlar. Bu standartlar kurumların bir nevi güvenlik beyanı olarak algılanmaktadır. Yasalar ise firmaları ve kurumları çeşitli önlemler alma konusunda teşvik edici yönde hareket eder. Hasta verilerinin güvenliği ve gizliliği hakkında çıkarılan ağır cezai kanunlar şirketlerin bu alana gereken önemi vermesini ve gerekli tedbirleri almasını teşvik eder. Bu standartlardan bazıları aşağıda listelenmiştir;

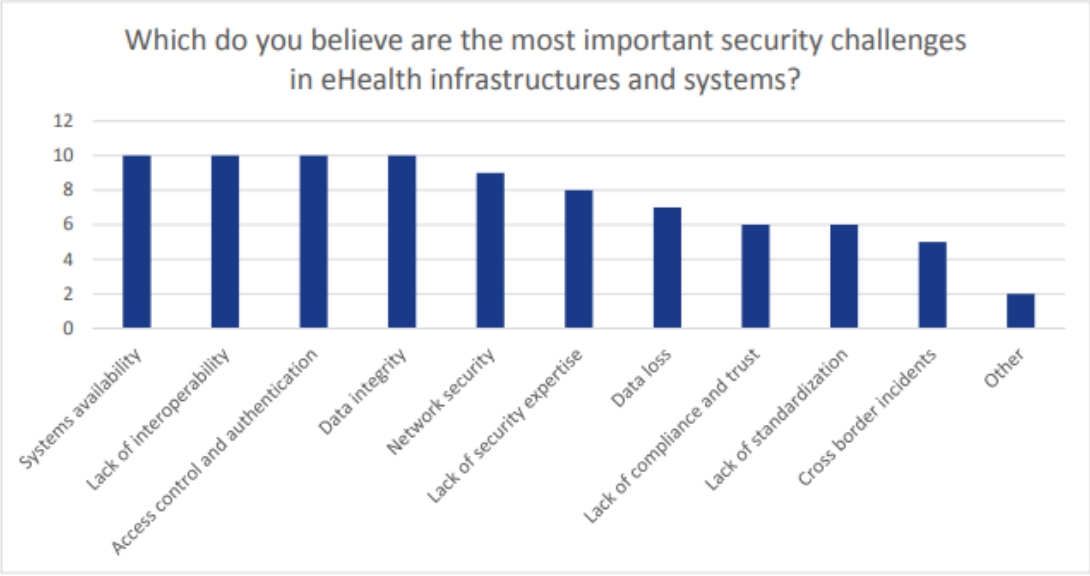
- ISO 18308:2011 (Health informatics -- Requirements for an electronic health record architecture)
- ISO/IEC 27000:2016 (Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary)

- IEC/NP 80001-1 (Safety, effectiveness and security in the implementation and clinical use of connected medical devices or connected health software -- Part 1: Application of risk management)
- ISO 27799:2016 (Health informatics -- Information security management in health using ISO/IEC 27002)

Dünya genelinde yasal çerçeve konusundan çalışma yapan bazı organizasyonlar şunlardır; HIPAA, HIMSS, Enisa, WHO, PAHO.

4.4.2 Teknik güvenlik

Güvenli bir e-sağlık sistemi için siber güvenlik savunma metotları elektronik sağlık mimarisindeki yazılım, donanım, ağ ve kriptografi gibi tüm bileşenlerinde uygulanmalıdır. Mimarinin herhangi bir yerinde bulunan bir güvenlik açığı saldırgan tarafından kullanılarak sisteme sızılabilir veya veriler çalınabilir. Bu sebeple teknik açıdan güvenlik düşünülürken bütüncül bir yaklaşım sergilenmeli her bir parçaya gereken önem verilmelidir. ENISA tarafından Avrupadaki sağlık kurumlarında yapılan bir araştırma sonuçlarına göre sağlık kuruluşları için balışa problemler erişilebilirlik, birlikte çalışma zorluğu, veri bütünlüğü ve kullanıcı yönetimidir[21]. Şekil 4.2'de bu araştırmanın sonuçları paylaşılmıştır. Amerika Birleşik Devletlerinde yapılan başka bir araştırmaya göre 2015 yılında farklı sağlık kurumlarından elektronik sağlık verisi çalınanların toplam sayısı 111 milyondur. Bu rakam ABD nüfusunun yaklaşık %35'i civarındadır.



Şekil 4.2: ENISA araştırma sonuçları[21].

4.4.3 Elektronik sağlık için güvenlik gereksinimleri

Bir elektronik sağlık sisteminin güvenliğinin sağlanabilmesi için yerine getirilmesi gereken bir takım gereksinimler vardır. Bu gereksinimler birkaç başlık altında toplanabilir.

- Vaka Yönetimi
    - Vakaları yönet
    - Vakaları ölçümle ve resmi olarak raporla
    - Vakalar için yardım masaları oluştur
    - Geri bildirimlere göre güvenliği geliştir
- Fiziksel ve Çevresel Güvenlik
    - Sunucuları ve ağ cihazlarını içeren veri merkezlerini güvenli bölgelere kur
    - Yetkisiz erişime karşı güvenlik tedbirleri al
    - Çevresel felaketlere karşı tedarikli ol
    - Kritik verileri takip et
    - Kapalı devre görüntüleme sistemleri kullan

- Ağ Güvenliği
    - Ağ topolojisinde bulunan tüm cihazların operasyonel güvenlik standartlarını karşıladığından emin ol
    - IPS ve IDS gibi sistemleri ağ mimarinden uygun yerlerde kullan
    - SSL/TLS gibi güvenli veri aktarım yöntemlerini tercih et
- Erişim Denetimi
    - Her hasta için tekil referans tanımla
    - Sadece yetkili kişilerce erişim hakkı tanı
    - Merkezi bir yetki otoritesi kur
    - Rol bazlı yapıda çalış

    - Loglama yap
    - Yetki seviyesine uygun veri sınıflama
- Erişilebilirlik ve Felaket Senaryosu
    - Düzenli yazılım ve veri tabanı yedekleri al
    - Operasyonel yapılandırma dosyalarının yedeğini al
    - Veri merkezi olarak yedekli bir yapı kur
- Farkındalık ve Eğitim
    - Çalışanları elektronik sağlık bilgi güvenliği konusunda eğit
    - Bilgi güvenliği süreçleri hakkında bilgi birikim düzeyini arttır
    - Televizyon ve diğer kitle iletişim yöntemleri ile toplumsal farkındalığı arttır
- Risk Yönetimi
    - Kritik varlıkları ve potansiyel tehlikeleri tanımla
    - Riskleri analiz et
    - Olası vakaların sağlık hizmetinde ve hasta güvenliğindeki etkilerini hesapla

5. ETHERUM İLE DAĞITIK ELEKTRONİK SAĞLIK UYGULAMASI

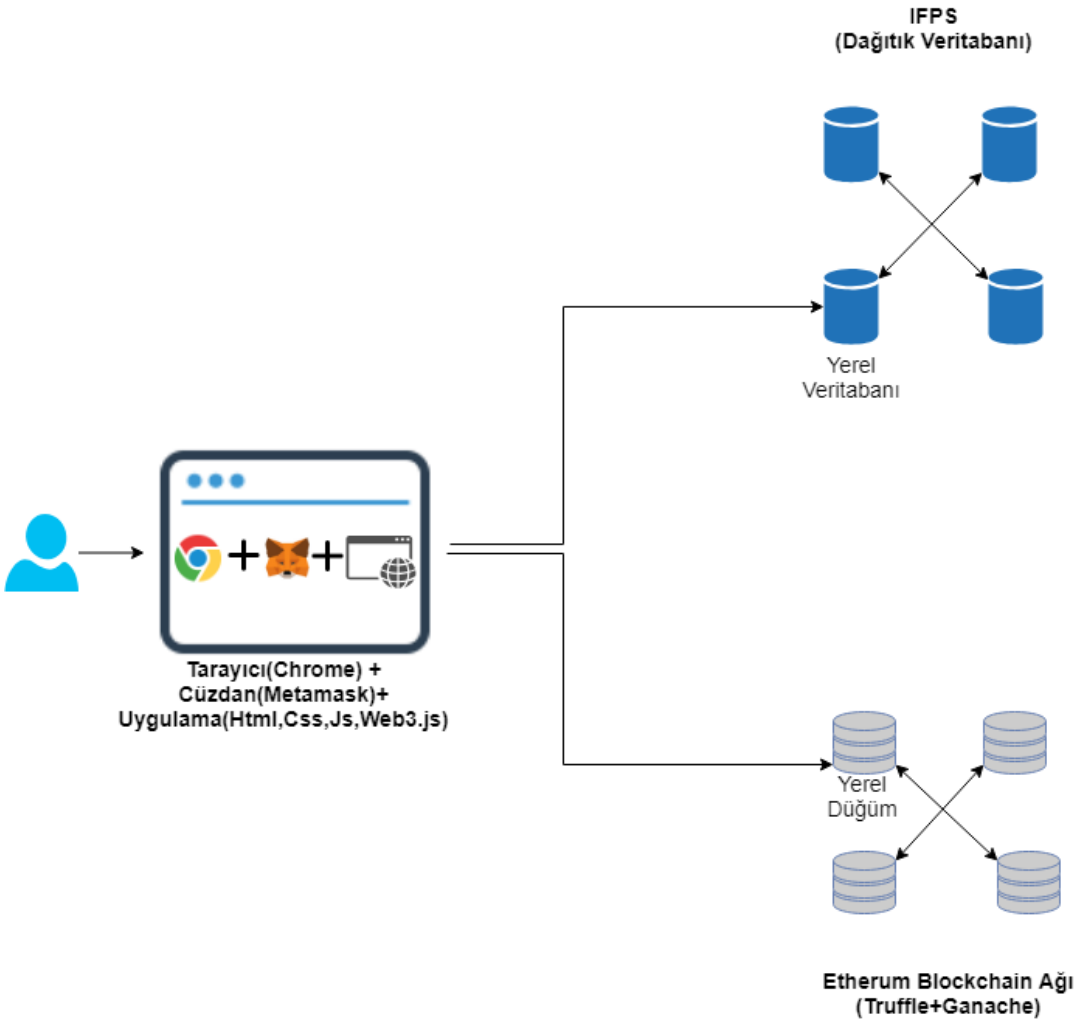
Elektronik sağlık sistemlerinin en öncelikli güvenlik problemlerinin başında hastalara ait elektronik sağlık verilerinin gizliliği ve bütünlüğü gelmektedir. Bu uygulama ile blockchain teknolojisi kullanılarak elektronik sağlık sistemlerinin problemlerine çözüm önerisi sunulmuştur. Verinin gerçek sahipliği kavramı dijital ortama uyarlanarak hastanın izni olmadan sağlık verisinin başkaları tarafından görüntülenmesinin önüne geçilmiştir. Ayrıca veri bütünlüğü açısından hastaya ait veriler üzerinde geçmişe yönelik manipülasyonları engelleyecek bir yapı kurulmuştur.

Uygulama geliştirilirken blockchain teknolojisi olarak Etherum tercih edilmiştir. Etherum akıllı sözleşmeler aracılığıyla blockchain düğümleri üzerinden dağıtık programcıklar çalıştırmanıza izin veren bir teknolojidir. Uygulamanın mantıksal iş katmanı blockchain üzerinde geliştirilmiştir. Herhangi bir merkezi sunucu taraflı bir uygulama veya web servisi kullanılmamıştır. Hasta kayıt etme, hasta bilgi girişi, hasta bilgi okuma gibi tüm akışlar blockchain akıllı sözleşmeler katmanında programlanmıştır. Önyüz uygulaması olarak web uygulaması geliştirilmiştir. Web uygulaması ile blockchain arasındaki iletişim web3.js kütüphanesi ile sağlanmıştır. Ayrıca karmaşık ve büyük verilerin tutulması için dağıtık veri tabanı teknolojisi olarak ifps kullanılmış ve bu veri tabanlarında hasta verilerinin şifrelenmiş versiyonları saklanmıştır.

5.1 Uygulama Mimarisi

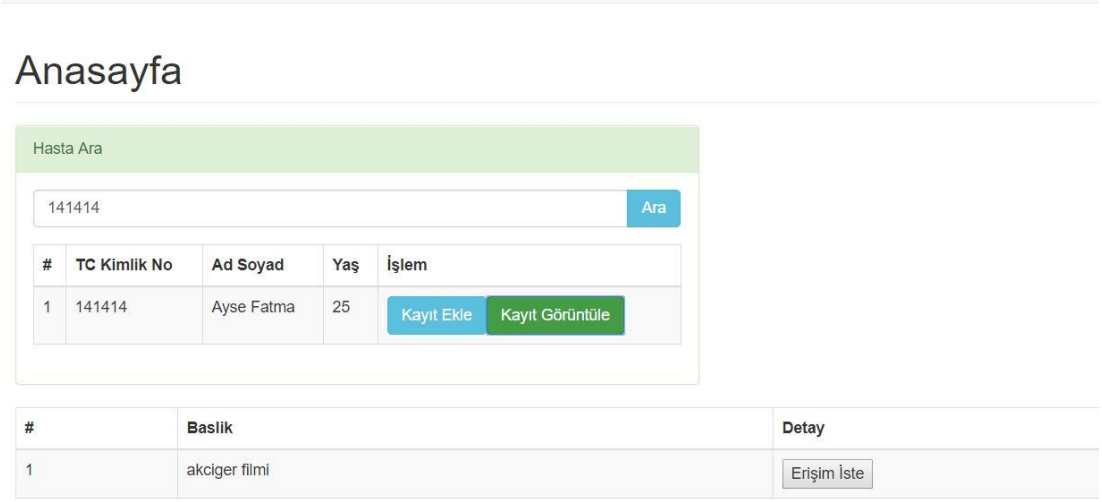
Uygulama mimarisinin görselleştirildiği çizim şekil 5.1'de verilmiştir. Önyüz uygulaması web projesi olarak geliştirilmiştir. Bu web projesinde oturum açan kullanıcıların doğrulanması amacıyla cüzdan uygulaması olarak çalışan metamask tarayıcı eklentisi tercih edilmiştir. Hastanın açık anahtarı ile şifrelenen hasta verilerinin şifrelenmiş halleri dağıtık veritabanlarında tutulmuştur. Dağıtık veritabnlarındaki belgelerin özet bilgileri referans olarak etherum blockchain ağında saklanmıştır. Veri okuma ihtiyacında önyüz uygulaması aracılığıyla ilgili verinin blockchain ağındaki

özet bilgisi elde edildikten sonra bu özet bilgiye karşılık gelen veri dağıtık veritabanından çekilmektedir. Veritabanından alınan şifrelenmiş bu veri son olarak alıcının saklı anahtarı ile çözülerek okumaya hazır hale getirilmektedir.



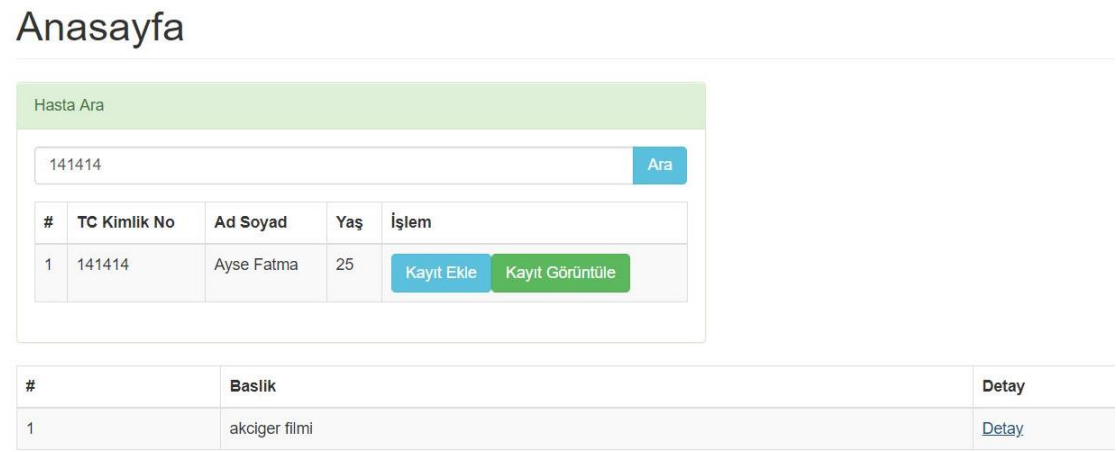
Şekil 5.1: Uygulama mimarisi.

Hasta bilgileri, doktor bilgileri, veriler üzerindeki izin istekleri ve izinler blockchain ağında akıllı sözleşmeler ile yönetilirken sağlık verilerinin şifrelenmiş versiyonları dağıtık veritabanında tutulmaktadır. Bir doktor herhangi bir hastanın verisini görüntülemek istediğinde akıllı sözleşmeler aracılığıyla öncelikle ilgili isteği arayüz uygulamasından hastaya göndermek zorundadır. Hasta isteğe olumlu yanıt verdiği takdirde ilgili doktor veriyi görüntüleyebilmektedir. Şekil 5.2'de hasta verisine erişim isteği yapılan ekran gösterilmektedir.



Şekil 5.2: Veri erişim isteği

Hastanın erişim isteğine onay vermesi sonrası doktor aynı ekranda oturum açtığında ilgili veriyi görebilmektedir. Şekil 5.3'te onay sonrası ekran görünümü gösterilmiştir.



Şekil 5.3: İzin sonrası görünüm

Doktor detay seçeneğine bastığında sisteme örnek olarak yüklenmiş akciğer filmini başarılı şekilde görüntülemektedir. Detay sonrası görünüm şekil 5.4'te verilmiştir.

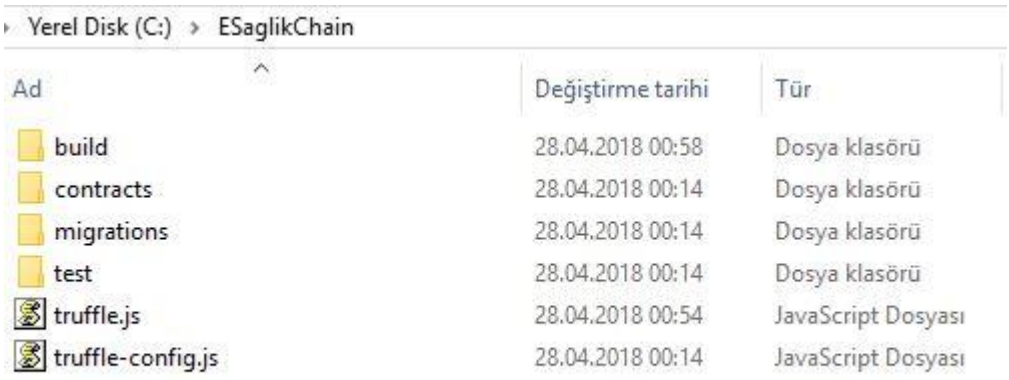
Şekil 5.4: Örnek akciğer filmi

5.2 Etherum Blockchain Ağı

Dağıtık uygulamanın iş katmanı Etherum blockchain teknolojisi kullanılarak geliştirilmiştir. Bu katman özel bir blockchain ağından ve akıllı sözleşmelerden meydana gelmektedir. Blockchain ağının her bir düğümü elektronik sağlık sistemine dâhil olan hastaneleri temsil etmektedir. Sisteme katılmak isteyen sağlık kuruluşları yetkili makamlardan izin aldıktan sonra kendi blockchain cihazlarını ağa ekleyerek bir düğüm haline gelmektedirler. Ağa katılım için gerekli olan yapılandırma ayarları yetkili makam tarafından sağlık kuruluşuna sağlanmaktadır.

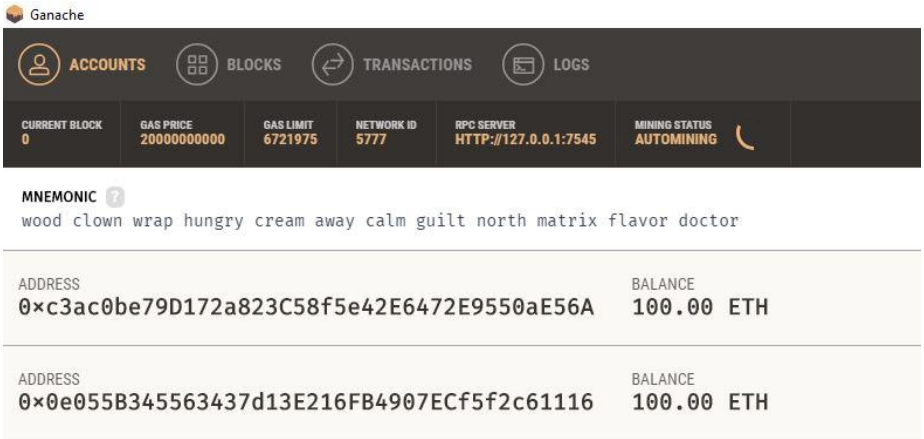
Etherum blockchain ağı kurulumu için Truffle kütüphanesinden faydalanılmıştır[22]. Truffle kütüphanesi etherum blockchain ağı kurulması, akıllı sözleşme geliştirmesi, akıllı sözleşmelerin derlenerek ağa yüklenmesi ve test edilmesi yönleriyle blockchain geliştirmeleri konusunda yazılım geliştiricilere kolaylıklar sağlayan bir kütüphanedir. Bu kütüphanenin özelliklerinden faydalanılarak süreçler hızlandırılmıştır. Kütüphane

dokümanları incelenerek ESaglikChain projesi oluşturulmuştur. Projenin klasör yapısı şekil 5.5'te gösterilmiştir.



Şekil 5.5: Proje dosyaları.

Proje dizininde yer alan "contracts" klasörü akıllı sözleşmeler için ayrılmış bir dizindir. Uygulamamız için gerekli olan özellikleri barındıran akıllı sözleşme yazılarak bu dizin altına eklenmiştir. Akıllı sözleşme geliştirilirken Solidity dili kullanılmıştır. Etherum blockchain ağı kurmak için Ganache istemcisinden faydalanılmıştır[23]. Ganache sağlamış olduğu arayüzler sayesinde özel bir blockchain ağını istediğiniz IP ve port üzerinde kısa sürede çalışır hale getirmenizi sağlamaktadır. Uygulamanın çalışacağı bu ağ oluşturulurken local ağ tercih edilmiştir. Ganache aracılığıyla ayrıca blockchain ağı üzerindeki hesaplar görüntülenebilir, işlemler takip edilebilir, bloklar ve madencilik durumu kontrol edilebilir. Ganache ile kurulan özel blockchain ağının arayüz görünümü şekil 5.6'da gösterilmiştir.



Şekil 5.6: Blockchain istemcisi.

Truffle tarafından oluşturulan ESaglikChain projesinin yaratılan bu blockchaine bağlanması için ip ve port yapılandırması truffle.js dosyasının içerisinde yapılmıştır. Yapılandırma aşağıdaki gibidir.

```
module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 7545,
      network_id: 5777
    }
  }
};
```

Konfigürasyon dosyasındaki değerler yerelde Ganache istemcisi ile oluşturulan blockchain ağının bilgileridir. Bu yapılandırmayla birlikte blockchain ağına bağlantı sağlanmıştır.

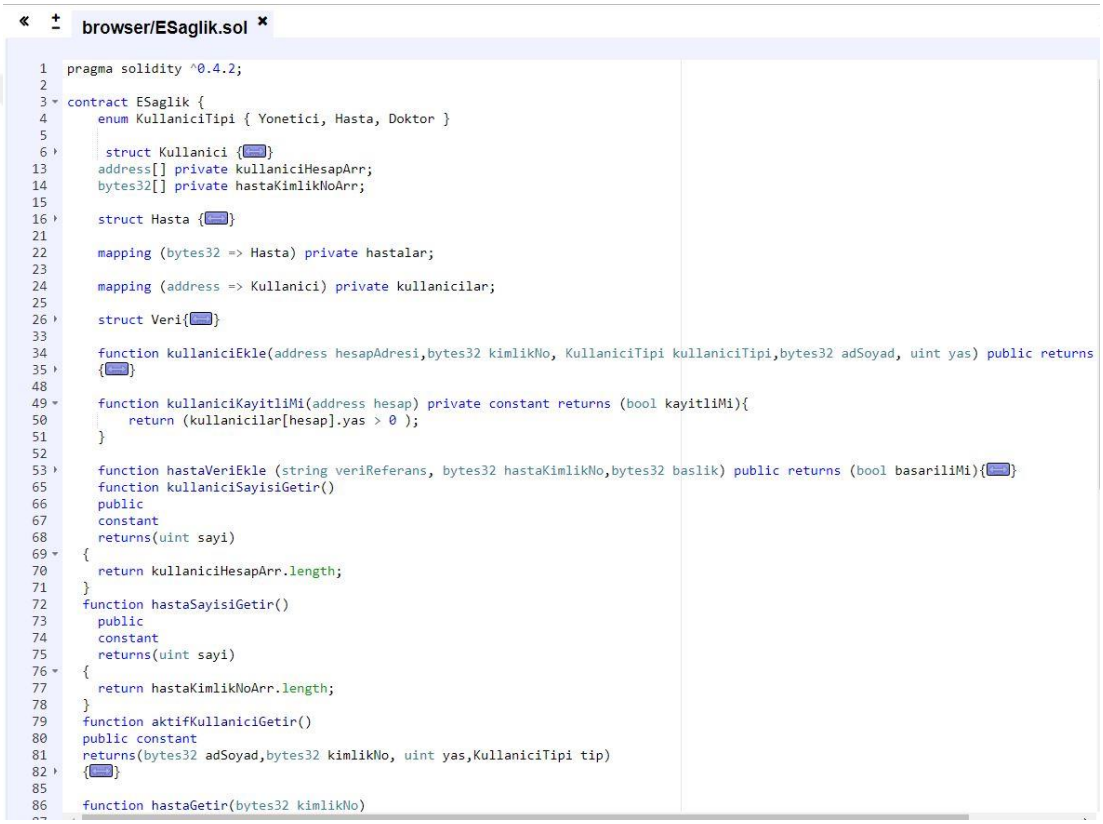
5.3 Akıllı Sözleşme

Dağıtık uygulamanın çalışacağı mantıksal iş katmanı solidty dilinde geliştirilmiştir. Solidty etherum blockchain teknolojisinde programlama dili olarak kullanılmaktadır. Akıllı sözleşmenin derlenmesi ve blockchain ağına yüklenmesi truffle kütüphanesi aracılığıyla yapılmıştır. Geliştirilen akıllı sözleşmenin sahip olduğu metotlar şunlardır;

- kullaniciEkle(address hesapAdresi, bytes32 kimlikNo, KullaniciTipi kullaniciTipi, bytes32 adSoyad, uint yas) public returns (bool basarili)
- kullaniciKayitliMi(address hesap) private constant returns (bool kayitliMi)
- hastaVeriEkle (string veriReferans, bytes32 hastaKimlikNo,bytes32 baslik) public returns (bool basariliMi)
- kullaniciSayisiGetir() public constant returns(uint sayi)
- aktifKullaniciGetir() public constant returns(bytes32 adSoyad,bytes32 kimlikNo, uint yas,KullaniciTipi tip)
- hastaGetir(bytes32 kimlikNo) public constant returns(bytes32 adSoyad,bytes32 retKimlikNo, uint yas)
- aktifHastaVeriGetir(uint indexVeri) public constant returns(bytes32 veriBaslik,string veriReferans,bytes32 yetkiIsteyen,uint index)
- hastaVeriSayisiGetir(bytes32 kimlikNo) public constant returns(uint sayi)

- hastaVeriGetir(uint indexVeri,bytes32 kimlikNo) public constant returns(bytes32 veriBaslik,string veriReferans, uint index)
- hastaVeriYetkiIste(bytes32 hastaKimlikNo,uint indexVeri) public returns(bool basariliMi)
- aktifHastaYetkiCevap(uint indexVeri,bool olumlu) public returns(bool basariliMi)

Bu metotlar önyüz uygulaması tarafından çağırılarak uygulamanın sahip olduğu iş akışı gerçekleştirilmiştir. Akıllı sözleşmenin kaynak kodunun bir kısmı görsel olarak şekil 5.7'de verilmiştir.



Şekil 5.7: Akıllı sözleşme kaynak kodu

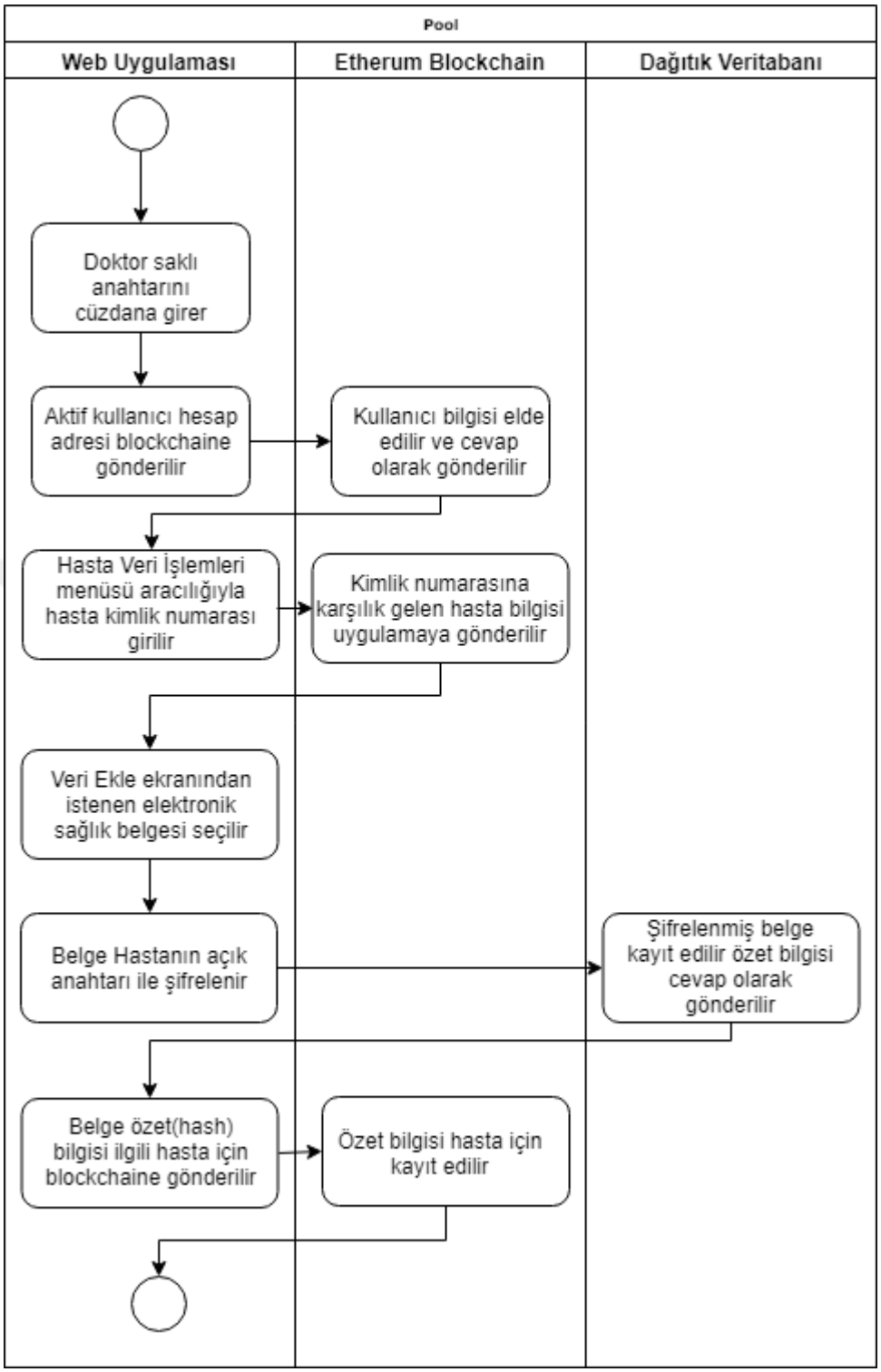
5.4 Önyüz Uygulaması

Uygulamanın kullanıcı arayüzü web uygulaması olarak geliştirilmiştir. Html5, css, javascript, jquery ve web3.js teknolojileri kullanılmıştır. Bu arayüz hem admin rolündeki yetkili kullanıcısı için hem de doktor ve hasta için tasarlanmıştır. Uygulamada her bir roldeki kullanıcılara yetki düzeylerine göre farklı menüler gösterilecek şekilde yetki kontrolü yapılmıştır. Admin rolündeki bir yetkili ile bir hasta

veya doktorun görebildiği arayüzler farklıdır. Yetki kontrolü yapılabilmesi için kullanıcılar tarayıcı eklentisi olan metamask cüzdana saklı anhatarlarını girdikten sonra sisteme oturum açmaktadırlar. Yetkisi doğrultusunda gerekli işlemleri yapan kullanıcıların arayüzle olan etkileşimleri web3.js kütüphanesi aracılığıyla blockchain ağına iletilmektedir. Web uygulamasının sahip olduğu kullanım senaryoları şunlardır;

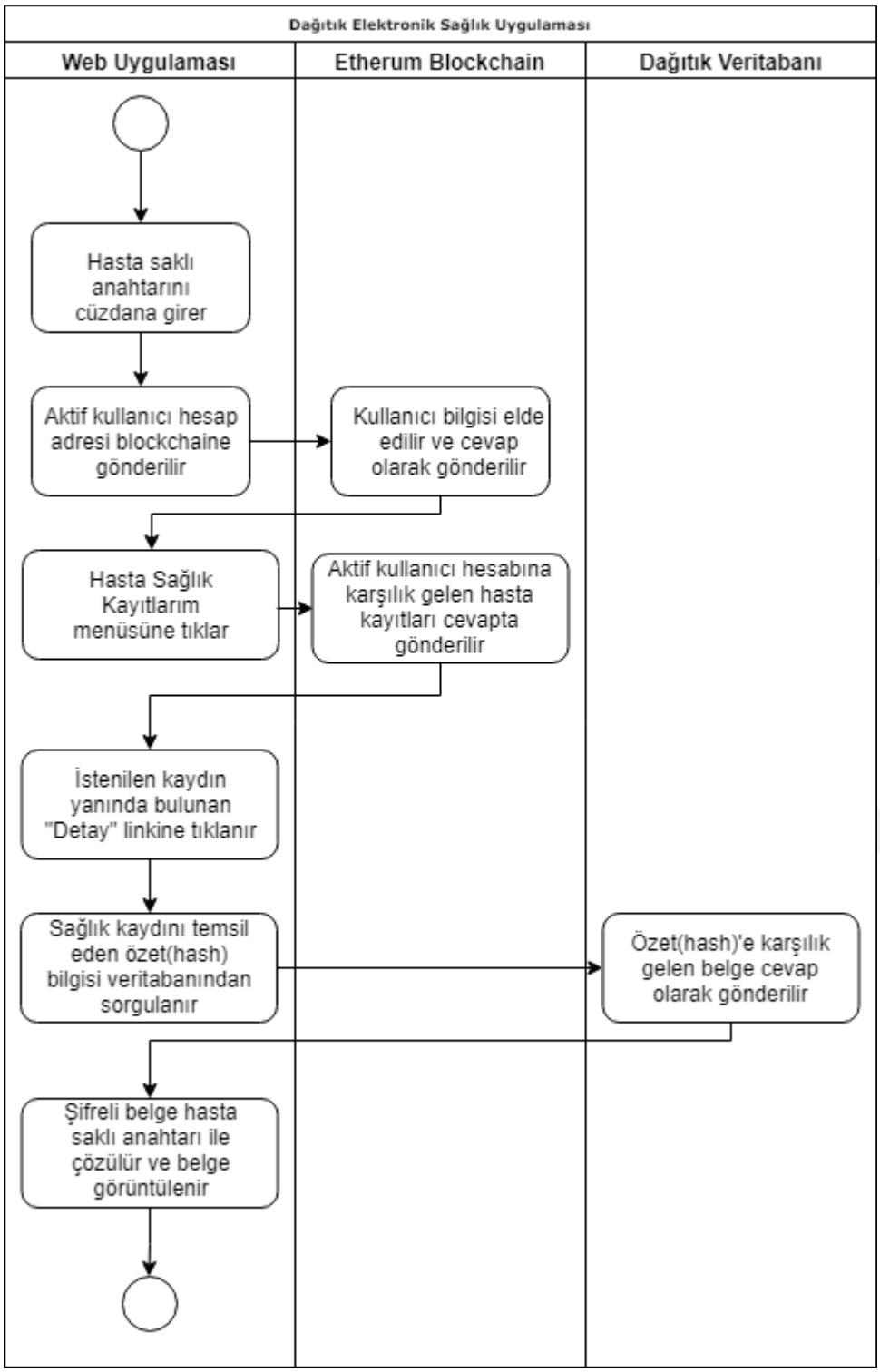
- Yönetici
    1. Kullanıcı sisteme giriş yapar.
    2. Kullanıcı Ekle menüsüne tıklar.
    3. İlgili formu doldurur ve onaylar.
    4. Uygulama akıllı sözleşmedeki ilgili metodu çağırır ve kullancı yaratılır.
    5. Blockchain tarafından eklenen kullanıcı için açık-saklı anhatar çifti yaratılır.
    6. Saklı anahtar ve hesap adresi kullanıcı ile paylaşılır.
- Doktor
    1. Sisteme giriş yapar.
    2. “Hasta Veri İşlemleri” menüsüne tıklar.
    3. İlgili hastayı kimlik numarası ile arayarak bulur.
    4. Hastaya ait olan veriyi sisteme yükler
    5. Yüklenen veri şifrelenerek dağıtık veritabanında kaydedilir.
    6. Şifrelenen verinin hash’i akıllı sözleşmedeki de ilgili metot çağırılarak blockchain üzerine kayıt edilir.
- Hasta
    1. Hasta sisteme giriş yapar.
    2. “Sağlık Bilgilerim” menüsüne tıklayarak kendisine ait bilgileri görüntüler.
    3. İlgili verilerin yan sütunlarında doktorlardan gelmiş bilgi paylaşımı isteklerini görüntülenir.
    4. Hasta uygun gördüğü isteği onaylar.
    5. Onaylanan veri ilgili doktor için erişilebilir hale gelir.

Şekil 5.8’de hasta için veri ekleme akış diyagramı gösterilmiştir.



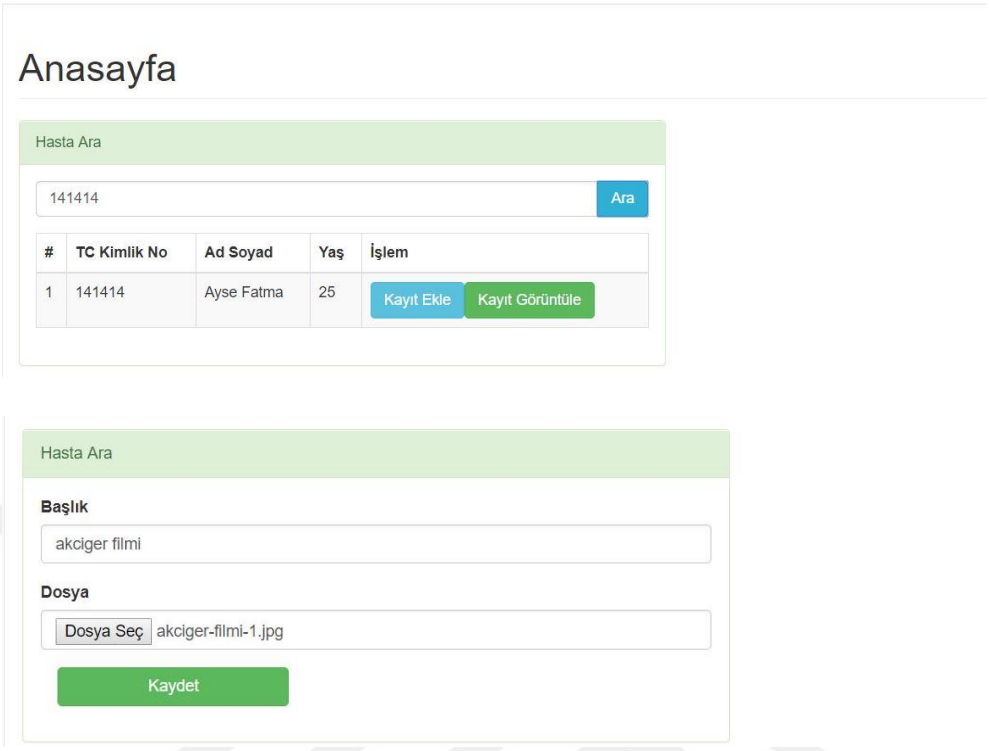
Şekil 5.8: Veri ekleme akış diyagramı

Şekil 5.9'da hasta veri okuma akış diyagramı gösterilmiştir.



Şekil 5.9: Veri okuma akış diyagramı

Şekil 5.10’da doktor tarafından veri eklemenin yapılacağı kullanıcı arayüzü gösterilmiştir.



Şekil 5.10: Doktor veri ekleme arayüzü

6. SONUÇ VE ÖNERİLER

Bu çalışma kapsamında etherum blockchain teknolojisi ve dağıtık veritabanı yapısı kullanılarak hasta sağlık kayıtlarının elektronik versiyonlarının tutulduğu dağıtık bir web uygulaması geliştirilmiştir. Blockchain teknolojisinin sahip olduğu temel özelliklerden faydalanılarak veri bütünlüğü ve gizliliği konusunda merkezi sistemlerle geliştirilmiş uygulamalara göre daha güvenli bir sistem oluşturulmuştur.

6.1 Kullanılan Yöntemler

Çalışma kapsamında öncelikle blockchain teknolojisi ile ilgili ayrıntılı bir teknik araştırma yapılmıştır. Teknolojinin sahip olduğu özellikler ve bileşenler incelenirken bu teknolojiye yön veren şirketlerden, araştırmacılardan ve uluslararası teknoloji kurumlarının kaynaklarından faydalanılmıştır. Elektronik sağlık sistemlerinin yapısı ve bileşenleri incelenerek sahip olduğu güvenlik problemleri araştırılmıştır. Güvenlik problemleri incelenirken çeşitli anket sonuçlarından ve araştırma raporlarından faydalanılmıştır.

Araştırmalar sonucu elde edilen bilgiler doğrultusunda uygun bir topoloji oluşturularak dağıtık bir elektronik sağlık uygulaması yazılım geliştirme süreçleri çerçevesinde geliştirilmiştir.

6.2 Elde Edilen Sonuçlar

Geliştirilen uygulama ile birlikte kişisel sağlık verilerinin gizlilik ve bütünlük açısından merkezi sistemlere göre daha güvenli bir şekilde saklandığı görülmüştür. Hastanın kendi verileri üzerinde söz sahibi olması ve kiminle paylaşılacağını kontrol edebilmesi kişisel verilerin korunması açısından hastayı daha güvenli hissettirmektedir. Verilerin şifrelenmiş hallerinin dağıtık veritabanlarında tutulması verilerin kötü niyetli kişiler tarafından görüntülenmesinin önüne geçmiştir. Ayrıca

şifreli verilerin özet karşılıklarının blockchain kayıt defterlerinde tutulması ile birlikte veri bütünlüğü sağlanarak geçmişe yönelik manipülasyonların önüne geçilmiştir.

Bu çalışma kapsamında daha genel amaçlarla üretilmiş olan etherum blockchain teknolojisi kullanılmıştır. Etherum teknolojisinin sahip olduğu özellikler kapsamlı bir elektronik sağlık sisteminin bütün ihtiyaçlarına cevap verecek düzeyde değildir. Yapılacak araştırmalarla birlikte ileri çalışmalarda elektronik sağlık sisteminin tüm ihtiyaçlarını karşılayabilecek yeni bir blockchain teknolojisi geliştirilebilir. Geliştirilen bu yeni blockchain teknolojisi kullanılarak üretilecek dağıtık elektronik sağlık uygulamasına web ve mobil önyüzler geliştirilerek sağlık sektörünün içerisindeki tüm aktörlere hizmet verecek bir sistem yaratılmalıdır. Ayrıca giyilebilir sağlık teknolojilerinden faydalanılarak bu sisteme veri girişinin yapılması da ileri çalışmalarda ele alınması gereken konular arasındadır.

KAYNAKLAR

[1] Topscott, A., & Topscott D. (2016). *Blockchain revolution : How the technology behind bitcoin and other cryptocurrencies is changing the World*. New York: Penguin

[2] Nakamoto, S. (2008). *Bitcoin: a peer-to-peer electronic cash system*. Alındığı tarih: 23.04.2018, adres: https://bitcoin.org/bitcoin.pdf

[3] Haber, S., & Stornetta, W.S. (1991). *Journal of croptology*. (ss. 99-111)

[4] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). *Blockchain technology overview*. Alındığı tarih: 01.03.2018, adres: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.9)

[5] Washington, L., & Trappe, W. (2002). *Introduction to cryptography: with coding theory*. Londra: Pearson. (s.5)

[6] İTÜ BİDB (2013). *Şifreleme yöntemleri.* Alındığı tarih: 10.02.2018, adres: https://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri

[7] Merkle Tree (t.y). In *Wikipedia.* Alındığı tarih: 15.02.2018, adres: https://en.wikipedia.org/wiki/Merkle_tree

[8] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). *Blockchain technology overview*. Alındığı tarih: 01.03.2018, adres: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.23)

[9] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). *Blockchain technology overview*. Alındığı tarih: 01.03.2018, adres: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.27)

[10] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). *Blockchain technology overview*. Alındığı tarih: 01.03.2018, adres: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.31)

[11] Blockchains & Distributed Ledger Technologies (t.y.). Alındığı tarih: 06.02.2018, adres: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[12] Types-of-Blockchains (t.y.). Alındığı tarih: 04.03.2018, adres: https://media.blockchainhub.net/wp-content/uploads/2016/07/Types-of-Blockchains-1.jpg

[13] R3 (t.y.). Alındığı tarih: 04.04.2018, adres: https://www.r3.com/about/

[14] Furlonger, D., & Valdes, R. (2017). *Practical blockchain: a Gartner trend insight report.* Alındığı tarih: 02.02.2018 adres: https://haas.campusgroups.com/ htc/get_file?eid=139611897577441f06512fc062b0a63e

[15] Kaminska, I. (2015). *Blockchain promises back-office ledger revolution.* Alındığı tarih: 20.03.2018 adres: https://www.ft.com/content/7aad0826-638c-11e5-9846-de406ccb37f2

[16] Belinky, M., Rennick, E., & Veitch, A. (2015) *The fintech 2.0 paper: rebooting financial services.* Alındığı tarih: 25.03.2018 adres: https://www.finextra.com/ finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf

[17] Treat, D., Brodersen, C., Blain, C., Kurbanov, R. (2017). *Banking on blockchain.* Alındığıtarih: 15.02.2018, adres: https://www.accenture.com/ t20171108T095421Z__w__/usen/_acnmedia/Accenture/Conversion-Assets/DotCom /Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50

[18] Deloitte (2017). *Evulation of blockchain technology.* Alındığı tarih: 05.01.2018, adres: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Evolution-of-blockchain.pdf

[19] State of Dapps (t.y.). Alındığı tarih: 19.02.2018, adres: https:// www.stateofthedapps.com/dapps

[20] World Health Organization (t.y.). Alındığı tarih: 25.02.2018, adres: http://www.who.int/ehealth/en/

[21] Liveri, D., Sarri, A., Skouloudi, C. (2015). *Security and resilience in eHealth.* Alındığı tarih: 15.01.2018, adres: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

[22] URL-1 <*http://truffleframework.com/docs/*>, alındığı tarih: 20.04.2018

[23] URL-2 < *http://truffleframework.com/ganache/*>, alındığı tarih: 20.04.2018

ÖZGEÇMİŞ

Ad Soyad **:** Mehmet MURAT

Doğum Yeri ve Tarihi : 12/12/1990, Beyoğlu

E-Posta **:** mrtmehmet@gmail.com

ÖĞRENİM DURUMU:

Lisans **:** İTÜ Elektronik Mühendisliği

Yüksek Lisans **:** Bilgi Güvenliği Mühendisliği ve Kriptografi

MESLEKİ DENEYİM :

Sim Yazılım ve Bilişim Hizmetleri - Yazılım Mühendisi (Mart 2018 - …)

Softtech A.Ş. - Yazılım Mühendisi (Temmuz 2015 - Mart 2018)

İTÜ BİDB - Yazılım Mühendisi (Şubat 2014 – Temmuz 2015)

İTÜ BİDB – Asistan Öğrenci (Nisan 2011 – Şubat 2014)