T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRKİYE'DE DİJİTAL ESERLERİN KORUNMASINDA BLOK ZİNCİRİ TASARIMI VE UYGULAMASI

Muhammet Mustafa TOZLU

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Temmuz-2022
KONYA

TEZ KABUL VE ONAYI

Muhammet Mustafa TOZLU tarafından hazırlanan "Türkiye'de Dijital Eserlerin Korunmasında Blok Zinciri Tasarımı ve Uygulaması" adlı tez çalışması 06/07/2022 tarihinde aşağıdaki jüri tarafından oy birliği ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Prof. Dr. Fatih BAŞÇİFTÇİ	……..
Danışman Doç. Dr. Mesut GÜNDÜZ	……..
Üye Prof. Dr. Mustafa Servet KIRAN	……..

Yukarıdaki sonucu onaylarım.

Prof. Dr. Saadettin Erhan KESEN
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Muhammet Mustafa TOZLU

Tarih:

ÖZET

YÜKSEK LİSANS TEZİ

TÜRKİYE'DE DİJİTAL ESERLERİN KORUNMASINDA BLOK ZİNCİRİ TASARIMI VE UYGULAMASI

Muhammet Mustafa TOZLU

Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Mesut GÜNDÜZ

2022, 69 Sayfa

Jüri
Doç. Dr. Mesut GÜNDÜZ
Prof. Dr. Fatih BAŞÇİFTÇİ
Prof. Dr. Mustafa Servet KIRAN

Küreselleşen dünyada insanlar hayal güçlerini kullanarak birçok farklı fikir üretmektedir. Bazen bu fikirler; sözler, eylemler, yazılar, resim veyahut başka araçlarla dışarıya aktarılmaktadır. Zihinsel bir faaliyet olarak görülen bu değerler bir çaba ve gayretin ürünüdür. Ancak bu fikirlerin kimin ürünü olduğunu belirleyebilmek oldukça güçtür. Bir fikri emeğin kime ait olduğunun yanı sıra öncelik olarak kimin fikri emeğinin ilk olduğu da önemlidir. Benzer olan fikirlerin ilk kimin tarafından ortaya atıldığı, yani ilk fikir kimin sorusu gündeme gelebilmektedir. Bu sorunu çözebilmek için bu tez çalışmasında blok zincirinin sağlamış olduğu zaman damgası ile bu soruna bir çözüm önerilmiştir.

Uygulama önerisinde blok zincirine eklenen örnek verilerin, zaman damgalı olarak tutulması gerçekleştirilmiştir. Bu dosyalar blok zincirine eklenirken eser sahiplerinin isimleri ile kaydedilmiş ve ayrıca doğrulama komutları çalıştırılmıştır. Direkt erişim ile eser sahibi ve ne zaman üretildiği bulunmuştur. Bu çalışmanın amacı fikri emek ile üretilen dijital eserlerin değiştirilemez ve zaman damgalı bir şekilde kime ait olduğunu ve ne zaman üretildiğini blok zinciri ile koruma altına almaktır. Böylelikle kişiler kendi fikri emeklerini ispat ederek fikri ve ekonomik haklarını koruyabileceklerdir.

Bu çalışma da blok zinciri üzerinde akıllı sözleşme oluşturulmuştur. İmzalama sertifikaları kullanılmadan JSON Web Token (JWT) yapısındaki belirteçler kullanılmış ve ek belirteçler oluşturulmuştur. Oluşturulan JWT yapısı ECDSA şifreleme algoritması kullanılarak şifrelenmiş ve bir kanıt dosyası üretilmiştir. Sertifika sunucuları aradan çıkartılarak ek işlem yükleri de kaldırılmıştır. Merkezi olmayan uygulamalar (DApp) ile oluşturulan kanıt dosyası blok zinciri üzerinden doğrulanarak dijital eserin bütünlüğünün, doğruluğunun ve değiştirilemezliğinin garanti altına alınması sağlanmıştır. Bu kanıt dosyasının adli sürece de yardımcı olabileceği düşünülmektedir.

Anahtar Kelimeler: Blok zinciri, Dijital Eser Korunması, Fikri Mülkiyet, Zaman Damgası, Dijital İmzalama Algoritması

ABSTRACT

MS THESIS

BLOCKCHAIN DESIGN AND IMPLEMENTATION FOR THE PROTECTION OF DIGITAL ARTIFACTS IN TURKEY

Muhammet Mustafa TOZLU

Konya Technical University
Institute of Graduate Studies
Department of Computer Engineering

Advisor: Assoc. Prof. Dr. Mesut GÜNDÜZ

2022, 69 Pages

Jury
Assoc. Prof. Dr. Mesut GÜNDÜZ
Prof. Dr. Fatih BAŞÇİFTÇİ
Prof. Dr. Mustafa Servet KIRAN

In the globalizing world, people produce many different ideas by using their imaginations. Sometimes these ideas are expressed by words, actions, writings, pictures or other means. These values, which are seen as a mental activity, are the product of great efforts. However, it is very difficult to determine whose product these ideas are. In addition to who owns that intellectual effort, it is also important to know who first produced it. Questions such as, among similar ideas which person first came up with that idea may come to the fore. In order to solve this problem a timestamp provided by the blockchain is proposed in this thesis study.

In the proposed work, time-stamped keeping of sample data added to the blockchain has been realized. While these files were added to the blockchain, they were recorded with the names of the authors and also verification commands were run. With direct access, the owner of the work and when it was produced can be found. The purpose of this study is to protect the information about who owns the digital works produced with intellectual labor and when they were produced, by using the blockchain with unchangeable and time-stamped manner. Thus, individuals will be able to protect their intellectual and economic rights by proving their intellectual efforts.

In this study, a smart contract was created on the blockchain. Tokens in JSON Web Token (JWT) structure were used without using signing certificates and additional tokens were created. The created JWT structure was encrypted by using ECDSA encryption algorithm and a proof file was produced. By removing the certificate servers, additional processing loads were also removed. The proof file created with decentralized applications (DApp) is verified over the blockchain, ensuring the integrity, accuracy and immutability of the digital artifact. This evidence file may also help the forensic process.

Keywords: Blockchain, Digital Artifact Protection, Intellectual Property, Timestamp, Dijital Signing Algorithm

ÖNSÖZ

Günümüz teknolojisi ile artan dijital eserlerin başkaları tarafından kopyalanarak kendilerininmiş gibi kullanılabileceği düşünüldüğünden bu eserlerin kime ait olduğu ve ne zaman üretildiği önemli bir konu haline gelmektedir. Bu sebeple dijital eserlerin korunmasında blok zinciri uygulamasının kullanılma gereksiniminin doğmuş olacağı düşünülmüştür.

Bu tez kapsamı dijital eserlerin ilk kimin tarafından ve ne zaman üretildiğini kanıtlayabilmeyi hedef almıştır. Bir ihtilaf durumunda dijital eserin sahibini tespit etmeyi kolaylaştırmaktadır. Son zamanlarda popüler olan bir çalışma konusu olan blok zinciri, güvene dayalı olmayan bir ortamda güven inşa edebildiği ve manipülasyon riskini minimize ettiği için tercih edilmiştir.

Bu çalışmam boyunca bilgi ve desteğini benden hiçbir zaman esirgemeyen danışman hocam Sayın Doç. Dr. Mesut Gündüz'e, tez savunmasında eleştirileri ile tezin iyileştirilmesine katkı sunan tez savunma jüri üyeleri Prof. Dr. Fatih Başçiftçi ve Prof. Dr. Mustafa Servet Kıran'a teşekkür ederim. Ayrıca bu süreçte her zaman yanımda olan, her konuda beni cesaretlendiren ve hiçbir zaman desteklerini esirgemeyen canım aileme ve arkadaşlarıma teşekkür ederim.

Muhammet Mustafa TOZLU
KONYA-2022

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

Kısaltmalar

CA	:	Sertifika Otoritesi
DApp	:	Merkezi Olmayan Uygulama (Decentralized Application)
ECC	:	Eliptik Eğri Kriptografisi (Elliptic Curve Cryptography)
ECDSA	:	Eliptik Eğri Dijital İmza Algoritması
FSEK	:	Fikir ve Sanat Eserleri Kanunu
HMAC	:	Hash Tabanlı Mesaj Doğrulama Kodu (Hash-Based Message Authentication Code)
JWT	:	JSON Web Token
KAMU SM	:	Kamu Sertifikasyon Merkezi
PoS	:	Hisse Kanıtı (Proof of Stake)
PoW	:	İş Kanıtı (Proof of Work)
TSS	:	Zaman Damgası Sunucusu (Time Stamp Server)

1. GİRİŞ

Küreselleşen dünyada insanlar hayal güçlerini kullanarak birçok farklı fikir üretmektedir. Bazen bu fikirler sözlere, eylemlere, yazılara, resme veyahut başka araçlarla dışarıya aktarılmaktadır. Elbette bu dışa aktarımların tamamı bir bütün halinde değerlendirildiğinde insan düşüncesi ve fikirlerini kapsar. İnsanlar dışa aktarımlarını yaparlarken bir emek ve çaba göstermektedirler.

Eskiden yaygın olan fiziki işgücü hala devam etmekte fakat bunun yanında zihinsel ve fikri işgücü artış göstererek yeniçağı şekillendirmektedir. Fiziki işgücünün bir bedeli var iken zihinsel ve fikri bir emeğin bedelinin ve karşılığının da olması gerekir. Böyle bir durumda ekonomik değerinin varlığı ile karşılaşılır. Çünkü zihinsel bir faaliyet olarak görülen bu değerler bir çaba ve gayretin ürünüdür. Ancak bu fikirlerin kimin ürünü olduğunu belirleyebilmek oldukça güçtür. Çünkü bunun kanıtlanması gerekirken neyin ve nelerin kullanılması gerektiği düşünülmektedir. İşte burada bu fikri emeklerinin korunması için zaman damgası teknoloji ortaya çıkmıştır. Haber ve ark. tarafından dijital içeriklere zaman damgası uygulanma yöntemi hakkında güvenli bir modelden bahsetmişlerdir. Bu modelle beraber güvenilir bir sistemde ihtiyaç duyulan dijitalleştirme yapısı verilmiştir (Haber ve Stornetta, 1990).

Bunun gibi Kamu Sertifikasyon Merkezinin (KAMU SM) tarafından mahkemelerde geçerliliği bulunan sistemlerde mevuttur. Bu dijital eserler zaman damgasını verecek sunucuya gönderilmeden önce belgelerin dijital özet değeri çıkarılır. Çıkarılan dijital özet değeri, zaman damgası sunucularına gönderilir. Bu özet değeri ile zaman bilgisi birleştirilerek yeni bir değer oluşturulur. Bu değer sunucunun özel anahtarıyla imzalanarak bir zaman damgalı dosya üretilir (KAMU SM, 2021). Yalnız bu sistemler merkezi bir otoriteye ait olup güvenilirliği yalnızca merkezi otorite tarafından sağlanabilmektedir.

Zaman damgası sunucusu (TSS) güvenilir olup olmadığının garanti edilemeyeceğinden ve aynı zamanda burada yapılan değişikliklerin tespit edilmesinin mümkün olamayacağı yönünde tartışmalar vardır (Haber ve Stornetta, 1990). Bu tartışmalar sonrasında zincir yöntemi öne sürülmüştür. Böylelikle zaman damgalarına müdahale edebilmek için bir önceki zaman damgalarında değişiklik yapılması gerekecektir (Une, 2001). Bu yöntem blok zinciri yöntemine çok benzemektedir.

İşte burada merkezi bir otorite olmadan herkesin güvenebileceği, doğrulama işlemini yapabileceği şeffaf bir ortam kurmak gereklidir. Bu sebeple dijital eserlerin

korunmasında blok zinciri uygulamasını kullanma gereksiniminin doğmuş olacağı düşünülmüştür. Bu çalışma insanların fikirlerinin ürünü olan dijital eserlerin blok zinciri uygulamaları ile koruma altına alınmak ve kime ait olduğunu tespitini sağlamayı hedeflemiştir.

Artık fikri işgücünün gelişen teknoloji ile dijital ortamlara aktarımı mümkün hale gelmiştir. Dijital ortamda ise herkesin, her an her şeye ulaşma imkânı neredeyse sınırsız bir hal almıştır. Dolayısıyla bir fikrin ve zihinsel faaliyetin ve bunlardan üretilmiş değerlerin olması kötüye kullanmaya sebebiyet verebilmektedir. Bu çalışma da sunulacak model ile bu kötüye kullanımı önleme konusu ele alınacaktır.

Blok zincir uygulamalarının sağlamış olduğu birçok avantajlar vardır. Bu avantajlar dijital eser olarak üretilen fikri eser sahipliğini belirlemede kullanılacaktır. Bu uygulama modeli blok zincirinin sunmuş olduğu değiştirilemezlik ve dağıtık olma özelliği üzerine kurulacaktır. Değiştirilemezlik özelliği ile blok zinciri tabanında yer alan veriler güncellenemez, silinemez ve kalıcı olarak saklanır (Watanabe ve ark., 2015). Bazı saldırı çeşitleri ile bu mümkün olabilse de Bitcoin gibi yüksek değere sahip blok zinciri ağlarında manipülasyon ihtimalini minimize ettiği varsayılmıştır (Gipp ve ark., 2015). Dağıtık olma özelliğiyle de birden fazla kişide aynı verinin yer alması da doğruluğundan şüphe edilemeyecek olmasını sağlamaktadır. Bu uygulama modeli ile de dijital eserin ekonomik değerinin de korunması kolaylaşacaktır.

Dijital eserin kime ait olduğu tespit edilirken aynı zamanda bu korumanın ne zaman başladığı da önemlidir. Çünkü insanların birbirine benzer bir düşünce üretmesi olasılık dahilindedir. Ya da dijitalleşen dünyada erişim kolaylığı ile üretilmiş ancak korunmamış fikri eserlerin kopyalanması ile kime ait olduğunun saptanması zorlaşacaktır. Bu durumda bu fikrin kimin tarafından daha önce üretildiği sorunu oluşacaktır. Kripto para birimlerinin blok zincirlerinde gerçekleşen dijital veriler dijital eserlerin özet değerleri eklenmişse, merkezi olmayan güvenilir zaman damgası hizmeti olarak kullanılabilir (Clark ve Essex, 2012). Bu sayede blok zincirinin avantajı olarak görülen zaman damgalı olarak verilerin işlenmesi öncelik algısının da sonlandırması beklenmektedir. Eserin sahipliğinin yanı sıra üretildiği zaman diliminde ne olduğu tam olarak belli olacaktır. Koruma ikili olarak sağlanacaktır. Zaman damgalı olması bu eserlerin ne zaman üretildiğini ortaya koyan en önemli avantaj ve gerekliliktir. Çünkü bir fikri emeğin kime ait olduğunun yanı sıra öncelik olarak kimin fikri emeğinin ilk olduğu da önemlidir. Sağlanan korumada benzer olacak bir fikrin birbiri ile öncelik ve sonralık, yani ilk fikir kimin sorusu gündeme gelebilir. Geliştirilen model de blok zincirinin

sağlamış olduğu zaman damgası bu sorunu çözmektedir. Böylelikle koruma iki faktörlü şekilde gerçekleşmiş olacaktır. Aslında elde edilecek yöntem fikri eserlerin sahipliğini belirlemede, başkalarının bu eserleri kendisininmiş gibi göstermesinin önüne geçilmektedir. Çünkü birbirleri arasında ilk düşüncenin kimin tarafından bulunduğu sorunu da ortadan kalkmaktadır. Birbirine benzer nitelikteki fikri eserlerinde böylelikle birbirine karışması da son bulacağı düşünülmektedir.

Bu çalışma dijital eserlerin bütünlüğünü, doğruluğunu ve değiştirilemezliğini garanti altına alırken, zaman damgalı bir şekilde kime ait olduğunu ne zaman üretildiğini koruma altına almayı hedeflemiştir. Bu çalışma blok zinciri ile fikri emeklerin değiştirilemez ve zaman damgalı bir şekilde kime ait oldu ne zaman üretildiği koruma altına alınacak bir yöntem önermektedir. Böylelikle kişiler kendi fikri emeklerini ispat ederek ekonomik değerlerini koruyabileceklerdir. Yine bu çalışma adli sürece de yardımcı olabilecek niteliktedir. Bu çalışma sahipliği belirleyebilecek bir nitelikte olduğundan korumadan kimin faydalanacağı tespit edilebilir. Adli makamlardan da herhangi bir ihtilaf durumunda gerekli incelemelerin başlatılması konusunda öncülük edebilecek bir çalışmadır.

Tez altı bölümden oluşmaktadır. Birinci bölümde dijital eserler hakkındaki sorunlara değinilmiştir. Ayrıca tezin amacı, tezin önemi ve tezin organizasyonuna yer verilmiştir. İkinci bölümde dijital eserlerin korunması yöntemleri araştırılmıştır. Ayrıca blok zincirinin sağladığı güvenlik ve kullanıldığı alanlarda veri saklama, veri doğrulama, veri transferleri gibi konularda ele alınarak güven bu tez çalışmasına güven veren çalışmalarda incelenmiştir. Üçüncü bölümde blok zinciri teknolojisine ve kriptolojik yöntemlere yer verilmiştir. Bu tez çalışmasında kullanılan yöntemler incelenmiştir. Dördüncü bölümde ise yeni bir model tasarımı yapılmaya çalışılmış ve bunun uygulaması geliştirilmiştir. Beşinci bölümde önerilen çalışma için sonuçlara yer verilmiştir. Literatürden farkına ve sağladığı faydalara değinilmiştir. Altıncı bölümde ise genel tez çalışması değerlendirilmiştir. Ayrıca gelecek çalışmalar hakkında bilgi verilmiştir.

2. KAYNAK ARAŞTIRMASI

Literatürde dijital içeriklerin zaman damgası ile korunması hakkında çalışmalar mevcuttur. Bunun yanı sıra oluşabilecek sorunları ele alırken, merkeziyetsiz bir yapı içinde blok zincirleri önerileri de yapılmıştır. Blok zincirine ile ilgili güvenin ön planda tutulduğu birçok çalışma mevcuttur. Genel olarak bu çalışmalar incelendiğinde blok zinciri kripto para transferi dışındaki birçok çalışma da veri saklama, veri doğrulama, veri transferi gibi konular üzerinde çalıştığı görülmektedir bu sebeple literatürdeki çoğu uygulama blok zincirinin veri taşıyabilme özelliği hakkında çalışmalar da yapılmıştır. Bununla beraber TSS'lerde yapılan zaman damgalamalarının blok zincirine aktarılabilmek için gerekli güven veren çalışmalar aşağıda bahsedilmiştir.

Une (2001), çalışmasında TSS sistemlerinde zincir yöntemini önermiştir. TSS'ler için üretilen her zaman damgasında kullanılmak üzere bir önceki zaman damgasının özet değeri oluşturulup onunla üretilme modelidir. Damgalarda yapılacak en ufak müdahalede, zincirdeki tüm diğer damgaları etkileyeceği TSS'lerde oluşabilecek müdahaleleri minimize edilebileceği hakkında çalışmalar yapmıştır.

Clark ve Essex (2012), transfer edilen verinin (mesajın) ne zaman üretildiğini bilebilmek ve doğrulanabilmesi için çalışmalar yapmışlardır. Üçüncü bir kişi olmadan bir iş kanıtı (proof of work) protokolü kullanıp verinin üretildiği anda yaklaşık bir karbon tarihi verilebileceğinden bahsedilmiştir. Bu çalışma için Bitcoin ağının işlem gücünü kullanacak bir şekilde CommitCoin adında bir çalışma gerçekleştirmişlerdir.

Gipp ve ark. (2015), çalışmalarında piyasa değeri yüksek kripto para birimlerinde güvenliğin daha yüksek olabileceğinden bahsedilmiştir. Blok zincirindeki işlemleri manipüle etme olasılığının daha az ya da bulunmadığı varsayılmaktadır. Bundan dolayı da zaman damgalarını manipüle edilemediği varsayılmıştır. Bitcoin kripto para birimini kullanarak, merkezi olmayan güvenilir zaman damgası verilmesini konu almıştır.

Torun (2017), çalışmasında arazi sahipleri arasındaki meydana gelen sınırları ihlal etme durumunu yönetebilmek için bir blok zincir uygulama önerisinde bulunmuştur. Yapılan araştırmalar neticesinde tutarsız sınır tespitleri problemi çıkmış ve bu problemleri önleyebilmek için blok zinciri mimarisine dayanan bir yöntem öne sürülmüştür. Bu çalışma ile arazi sahipleri arasında yaşanan çatışmaları minimize hale getirmektedir. Tapu kayıt işlemlerinin merkezi sistem üzerinden kontrol edildiğini ve bu kontrolün blok zincirinin getirdiği avantaj ile tapu kayıtlarının merkezi sistem olmadan, şeffaf bir şekilde herkesin erişimine açık bir şekilde verilmesini önermiştir.

Ayberkin ve ark. (2018), çalışmalarında blok zincirinin özelliklerini ve işleyiş şekline değinilmiştir. Ayrıca bu çalışmanın amacı olan blok zinciri ile doğrulanabilir eğitim belgelerinden bahsedilmiştir. Blok zinciri yapısı nedeni ile verilerin saklanma şeklinden dolayı değiştirilmesinin imkansıza yakın olduğu ve bu özelliği ile eğitim belgelerinin nasıl güvenle saklanabileceği anlatılmıştır. Bu belgelerin güvenliğini sağlayabilmek ve gerçek zamanlı olarak bu belgeleri doğrulamayı gerçekleştirebilmek için blok zinciri üzerindeki bir model önerisi oluşturulmuştur. Bir blok zincir tabanlı uygulama kurgulanmıştır. Kurgulanan sistem modelinin güvenilir bir şekilde eğitim belgelerinin doğrulanabileceğinden bahsedilmiştir.

Hepp ve ark. (2018), geleneksel zaman damgalama yöntemleri yerine merkezi olmayan güvenilir zaman damgalama yöntemleri hakkında yöntemler ileri sürmüşlerdir. Telif hakkı ihlallerinde şüphe bırakmayacak şekilde kanıtlamasını sağlayabilmek için blok zincir temelli olarak belgelerin zaman damgalı olarak nasıl üretileceğini ve bunların nasıl doğrulanabileceği hakkındaki modelleri genişletmiş ve verimli hale getirecek önerilerde bulunmuşlardır.

Aydın (2018), seçim sistemlerinde kullanılması ile bizlere dijital oy imkânı sağlamakta ve dijital oyların imzalanarak doğrulanabileceğinden bahsetmektedir. Bu çalışma sayesinde online seçimlerde blok zinciri tabanlı seçim sistemlerini incelemiş avantajları ve dezavantajları ortaya koymuştur. Bu çalışmada verilerin güvenliğini sağlayabilmek için kriptolojik yöntemler araştırılmıştır. Bu yöntemler ile daha güvenli bir seçim sistemi kurulmaya çalışılmıştır.

Hasan ve Salah (2018), çalışmalarında dijital eserlerin müşteriye dağıtımı ve teslimi sırasında yaşanan zorluklar bahsedilmektedir. Burada yaşanan sorunlar ele alınarak bu sorunlar için blok zinciri kullanılarak bir teslim yöntemi sunulmuştur. Kullandıkları akıllı sözleşmeler ile müşteri, dijital içerik üreticisini ve bu dijital içeriği barındıran dosya sunucusu arasında bağ kurarak tüm etkileşimleri yönetmeyi hedef almıştır. Bir anlaşmazlık çıkması durumunda bunları çözmek için akıllı sözleşme düzenlenmiştir. Bu çalışmadaki dijital içerikleri oluşturan dosyalar ise blok zinciri dışında bulunan güvenli bir ortamdan indirilmesi sağlanmıştır.

Deniz ticaretinde özetle eşyaları temsil eden belgenin adına konşimento denmektedir. Bu belge ile denizde hareket eden gemilerle taşınan yüklerin sahipliği belgelenmektedir. Yıldız ve Baştuğ (2018), çalışmalarında blok zinciri temelli elektronik konşimentolar üzerinde çalışılmıştır. Bu çalışmayla elektronik konşimentoların hak sahipliğini blok zincirinin özellikleri arasında yer alan değiştirilememezlik yapısı ile

belirlenmekte ve deniz ticaretindeki eşyaların kaydının oluşturulması sağlanmaktadır. Ayrıca teslim işleminin daha pratik bir şekilde olması amaçlanmıştır. Böylelikle lojistik alanında evrak yükünün zorluklarının azaltılması ve işin gizliliğinin blok zinciri ile teminat altına alınabileceğinden bahsedilmiştir. Konşimentoların varlığı deniz ticareti için büyük önem taşımasından dolayı blok zinciri kullanılarak bu belgelerin güvenliğinin sağlanması ve transferinin yapılabileceği ileri sürülmüştür.

Blok zinciri teknolojisinin kullanılma amaçlarından biri de verilerin doğrulanabilir olması ve bu veriler eklendikten sonra bir daha geçmişe yönelik değiştirilemez oluşudur. Bununla ilgili bir çalışmada şu şekildedir. Yılmaz (2019), çalışmasında ürün tedarikindeki sürecin kolaylıkla kontrol edilebilmesi amaçlı takip uygulamasından bahsedilmiştir. Blok zinciri sisteminin nerelerde uygulanabileceği ve yüksek güvenlik sağlamak için kullanılan kriptografi işlemleri hakkında bilgilere değinilmiştir. Yine aynı şekilde blok zinciri teknolojisindeki güvenlik açıklarından biri olan %51 saldırısından bahsedilerek engellemek için yapılabilecek çalışmalar anlatılmaya çalışılmıştır. Ethereum teknolojisinden ve akıllı kontratlar bahsedilmiştir. Bir blok zinciri uygulaması yapılmış ve bu çalışma sonucunda blok zinciri teknolojisinin eklenen kayıtların değiştirilemez olmasının verdiği avantajla taraflar arasında güvenli alışverişinin yapılmasın mümkün olduğu gösterilmiştir.

Zhang ve ark. (2019), çalışmalarında dijital dosyalar için Chronos adında ileri sürdükleri blok zinciri ile güvenilir ve doğrulanabilir zaman damgalama şeması oluşturmuşlardır. Bu çalışmada dosyaların bir blok zincir üzerindeki zaman damgasını oluştururken Chronos Log Sunucuları üzerinden oluşturulmaya çalışılmıştır. Aynı zamanda bulut depolama da sunulmaktadır. Ethereum ağına entegre edilerek dosyaların zaman damgası eklenmesi sağlanmaktadır. Blok zincir kalitesi tutarlılığı hakkında da analizler yapılmıştır.

Dijital eserler arasına giren sertifikalar içinde doğrulanabilme ve kimin tarafından üretildiğinin bilgisinin bulunma ihtiyacı vardır. İkizoğlu (2019), çalışmasında üretilen diplomaların ve sertifikaların blok zincir üzerinde yönetimi yapılmıştır. Sahte belge üretiminin engellenmesi öngörülmüştür. Başka kurumlar ya da kişiler tarafından doğrulanması güç olan bu sertifika ve diplomalar için yine bu yöntem ile doğrulama işlemleri de yapılmıştır. Türkiye'de uygulanan yönetmelikler araştırılmış ve buna uygun Blockcerts mimarisi seçilerek bu yapı blok zinciri üzerine uyarlanarak bir metot geliştirilmiştir. Ayrıca blok zincirinin önemli yapan özelliklerinden de bahsedilmiştir.

Geleneksel yöntemler kullanıldığında veri manipüle edilebilir ya da bu veriler kaybolabilir. Bunlar için imzalama yöntemleri geliştirilmiş ve blok zincir yöntemi üzerinde bunlar imzalanarak geçerliliği korunmuştur. Bu içerikler içinde zaman damgası eklenerek takip edilebilen çalışmalar mevcuttur. Bu çalışmalar göz önüne alındığında dijital eserler içinde aynı koruma yöntemleri kullanılabilmektedir.

Gerdan (2019), çalışmasında geleneksel tedarik zincirinde meydana gelen bilgiler kaybolmakta olduğunu incelemiştir. Blok zincir teknolojisinin geleneksel tedarik zincirine getireceği faydalarından bahsedilmiştir. Bir organik yumurta üreticisi tasarlanıp blok zincir teknolojisi içeren bir dijital platform varsayılmıştır. Tasarlanan prototip ile yumurta üretim bilgileri çiftlikten sofraya kadar veri kaybı olmadan saklanmıştır. Bu çalışmada kullanılan akıllı sözleşmeler sayesinde gerçek zamanlı izlenebilirlik sunulmuş ve dijital imzalar sayesinde taraflar arasındaki iletişim güvenli bir hale getirilmiştir.

TSS'lerde gerçekleşen kimlik doğrulamasını blok zinciri üzerine taşınabileceğini gösteren çalışmalar mevcuttur. Altuncu (2019), çalışmasında blok zincir tabanlı bir platform olan Blockstack kullanarak kimlik doğrulama seremonisi için güvenlik anlamında daha iyi bir çözüm bulunmaya çalışılmıştır. Bu tez çalışmasında kimlik doğrulamaları sunucu taraflı tutulmasından ziyade blok zinciri kullanılarak doğrulanması sağlanmıştır. Bunların kullanılabilirliğini açıklamak içinde açık kaynak olan Signal Android Messenger uygulaması kullanılarak bir uygulama geliştirilmiştir. Bunlara ek olarak da tehdit modeli oluşturma ve güvenlik analizi yapılmıştır.

Kaya (2020), çalışmasında gayrimenkullerin akıllı sözleşmeler ile blok zincirine entegre oldukları varsayımında elde edilecek avantajların çokluğundan bahsedilmiştir. Söz konusu akıllı sözleşmeler ile gayrimenkulün üzerindeki işlemleri kolaylıkla halledilebileceklerdir. Akıllı sözleşmelerin uygulanması halinde evrak yükünün minimize edilmesinin yanı sıra blok zincirinin sağlamış olduğu özellikler neticesinde sözleşmedeki koşulların şeffaf ve açık olması sağlanmıştır. Bu sistem ile tarafların belirlemiş olduğu akıllı sözleşmelerdeki koşulların gerçekleşmesi halinde otomatik işlemlerinin yapılması ve koşulların taraflarca kontrolünün sağlanması mümkün hale geleceği belirtilmiştir. Akıllı sözleşmelerin sağlamış olduğu avantajlardan bir diğeri ise taraflara ödeme kolaylığı ve işlemlerde zamandan tasarruf oluşturacağından bahsedilmiştir. Yine blok zincirinin değiştirilemez özelliği ile tapu kayıtlarının güvenliği taahhüt altına alınabileceği konu edilmiştir. Bu çalışmayla beraber tapu gibi değerli evrakların blok zinciriyle korunabileceği anlatılmıştır.

Hyla ve Pejaś (2020), çalışmalarında dijital olarak imzalanan belgelerin yıllarca saklanabilmesi vurgulanmıştır. Dijital belgelerin imza geçerliliğinin uzun süre nasıl sağlanabilir olduğu incelenmiştir. Genellikle imzalarda açık anahtarın bulunduğu sertifika geçerli olduğu sürece bu imzalar geçerli kaldığından ve doğrulamayı daha uzun bir süreye taşımak için ek işlemler yapılması gerektiğinden bahsedilmiştir. Bu sorunları ele alarak bir Yuvarlak Tabanlı Blok Zinciri Zaman Damgalama Planı (Round-based Blokchain Time-stamping Scheme - RBTS şeması) çözüm modeli üretilmiştir.

Blok zincirinin adli süreçlerde kullanılabilmesini ve bu süreçte tüm belgelerin zaman sırasına göre erişilip güvence altına alınabileceğini gösteren bir başka çalışma ise Gündüzgil (2021)'in çalışmasıdır. Bu çalışma da elektronik delileri el koyma ve imaj alma aşamaları için yetki düzeyleri belirlenmiştir. Bu yetki düzeylerine göre blok zincir teknolojisi kullanılmış ve delillerin süreç yönetimi uygulaması ortaya konulmuştur. Bu uygulama sayesinde elektronik delillerin kayıt altına alarak adli sürecin başından sonuna kadar adli merciler ve kolluk kuvvetleri için silinemez ve değiştirilemez bir yapı ortaya konulmuştur. Uygulama için bir adli vaka konusu canlandırılmış ve canlandırılan bu kurgu için yapılan uygulamanın işlevleri kanıtlanmıştır.

Alyaz (2021), çalışmasında daha öncesinde manipüle edilmesi kolay olduğu için dijitalleşmeyen internet tabanlı oylama sistemlerinin, blok zincir teknolojisi kullanılarak geliştirildiğinde silinemeyen, değiştirilemeyen, zaman damgalı ve şifrelenmiş bir yapıya büründürerek dijital platforma dönüştürme önerisi sunmuştur. Gerçek zamanlı iletişim içinde WebRTC teknolojisi kullanmıştır. Güvenli, gerçek zamanlı dağıtık bir blok zinciri sistem mimarisi kurgulamıştır.

Ferwana (2021), çalışmasında verilen veya verilmesi düşünülen üniversite bursu veya bağışçıların vermek istediği bağışlara ilişkin olarak bağışçıların veya öğrencilerin burs ve bağışları şeffaf bir şekilde takip edebilmeleri amaçlanmıştır. Bu uygulama daha çok güven oluşturma üzerine kurulması planlanmıştır. Bağışçıların, öğrencilere bağışın ulaşma sürecini takip etmesi için blok zincir sistemi ile bağışların toplanmasında ve ulaştırılmasında görev alan aracılardan bağımsız bir sistem oluşturulmaktadır. Bağışçılar ve öğrenciler şeffaf bir şekilde bu bilgilere ulaşabilmektedir.

Aghayev (2021), yaptığı çalışmada telif haklarından ve yasal düzenlemelerden bahsetmiştir. Dijital eserlerin korumak için kullanılan teknik yöntemler anlatılmıştır. Yazılı eserleri dijital ortama aktarma ve eser sahibinin bu dijital haklarını nasıl yönetebileceği hakkında blok zinciri ile ilgili bir uygulama yapmıştır. Bu uygulamada eserler için sınırlı sayıda eser oluşturulmasına imkân sağlamıştır. İlk eser üretildiğinde

belli bir arz sınırı oluşturularak eserin değeri korumaya almaya çalışılmıştır. Eser metinleri blok zincirinde saklanmak için pahalı olduğundan harici bir depolama merkezi kullanılmıştır. Okuyucular NFT yani değiştirilemeyen token olarak isimlendirilen dijital kopyaları satın alabilmesi ve satın alma işlemi sonrasında sunucu üzerinden eser metnine erişim sağlayabilmesi hakkında çalışma yapmıştır. Eser sahiplerinin oluşturduğu akıllı sözleşme üzerinden arz miktarını geçmemek koşulu ile okuyucular token oluşturabilmekte ve ödenen ücret, bu akıllı sözleşme üzerinde biriktirilerek eser sahibine aktarılmaktadır. Bu uygulama eser sahibi ile okuyucu arasındaki bağlantıyı kurmasına ve aralarındaki ilişkiyi yönetmek ve okuyucuya özel bir dosya sunmayı hedef almıştır.

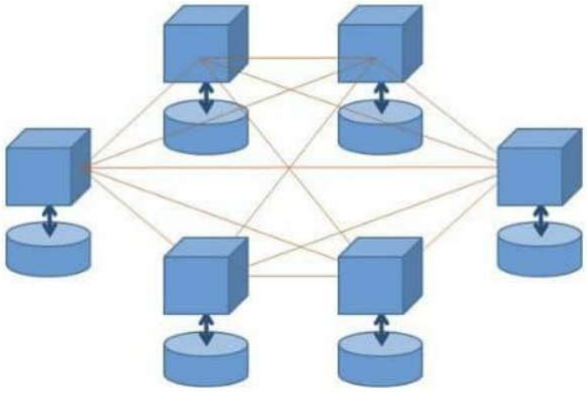
3. MATERYAL VE YÖNTEM

3.1. Blok Zinciri Teknolojisi

Blok zinciri kaydedilen bir verinin değiştirilemediği bu anlamda güvenilir bir yapıya sahip olan dağıtık veri kayıt sistemi olarak tanımlanabilir. Veriler kriptografik kanıtlarla kullanılarak birbiri ile kronolojik sıra gözetilerek bloklar halinde kaydedilir ve bu şekilde depolanır.

3.1.1. Blok zinciri yapısı

Blok zincirine kaydedilen bilgilere veri demekteyiz. Bu veriler saklandığı yapılara ise blok ismi verilmektedir. Böylelikle her veri bloğu kendisini tanımlayan özel bir dijital kimliğe sahiptir. Bloklarda verilerin ne zaman işlendiği bilgisi de kaydedilmektedir. Bu bloklar birbirini takip eden bir yapıya sahiptir. İlk blok, veri işlendikten sonra adeta mühürlenmekte ve daha sonra başka bir blok yanına eklenerek aynı şekilde devam etmektedir. İlk bloktan önce herhangi bir eşsiz dijital imza olmadığı için "Genesis" başlangıç bloku denir. Blok zincirinin sıralı yapısında diğer blok zincir bir önceki blokun dijital imzasını taşıması mümkündür. Şekil 3.1'de gösterildiği gibi aynı anda blok zincirde yapılacak ihlalleri ve oynamalara karşı güvenilirliği sağlayabilmek için blok zincirin kopyalarının herkese dağıtılmış olması sebebiyle dağıtık yapıdadır. Sisteme dahil olan herkese blok zincir dağıtılarak çoğunlukta yer alan bilgilerin doğru olduğunun kabulüyle koruma sağlar (Usta ve Doğantekin, 2017).



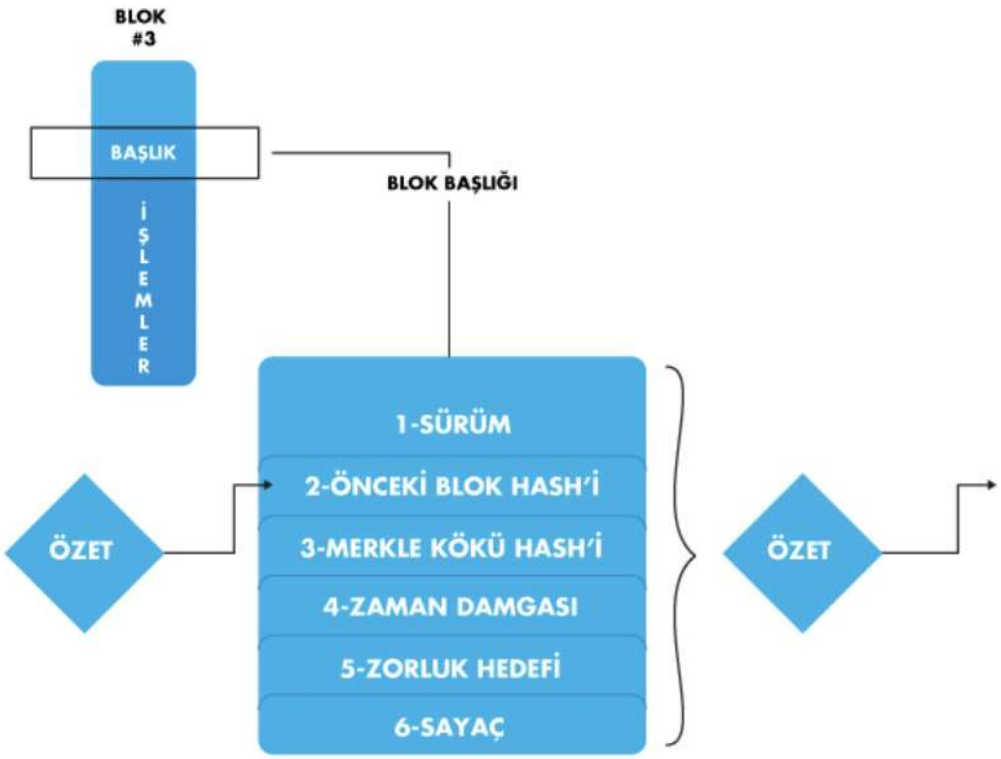
Şekil 3.1. Blok Zincirin Dağıtık Yapısı (Aydın, 2018)

3.1.1.1. Blok yapısı

Blok zinciri bloklardan oluşur. Her bloğun temel yapıtaşları mevcuttur. En temel yapıtaşları Blok Başlığı (Block Header) ve verilerin bulunduğu alan Blok Gövdesi (Block Body) olarak iki parçadan oluşmaktadır (Usta ve Doğantekin, 2017).

3.1.1.2. Blok başlığı (Header)

Temel olarak blok başlığında 6 ana bileşen bulunmaktadır (Gerdan, 2019). Bu bileşenler şekil 3.2'de gösterilmiştir.



Şekil 3.2. Blok Başlık Yapısı (Güven ve Şahinöz, 2018)

- Versiyon (Sürüm)
- Kendisinden önce gelen bloğa ait özet değeri
- Merkle kök değeri
- Zaman damgası
- Zorluk Hedefi
- Sayaç (Nonce)

3.1.1.3. Versiyon numarası (Sürüm)

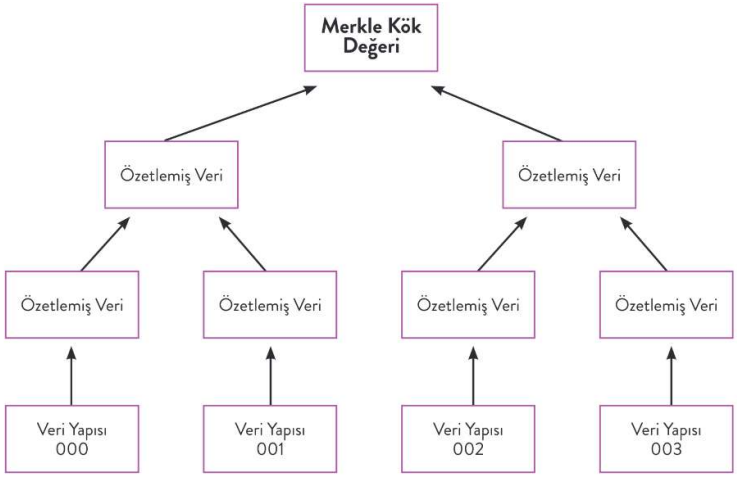
Blok zincirindeki hangi blok doğrulama kurallarının uygulanacağını göstermektedir (Zheng ve ark., 2017).

3.1.1.4. Kendisinden önceki bloğun özeti

Bu değer sayesinde kronolojik bir sıra oluşturarak bloklar arasındaki zincirin oluşmasını sağlamaktadır (Usta ve Doğantekin, 2017).

3.1.1.5. Merkle kök değeri

Büyük veri gruplarının güvenli ve hızlı doğrulanması amacıyla işleyen bir yapıdır. Bu yapıda ikili (binary) sistem kullanılmaktadır. Görüntü itibari ile ağaca benzediği için ağaç yapısı olarak adlandırılmıştır. Bu sistemde blok zincirlerine erişimi kolaylaştırmak için ikili bir şekilde veriler özetlenir. Daha sonra bu özetleme sonucu elde edilen değerler tek bir özetleme değeri elde edilinceye kadar ikili olacak şekilde özetlenmeye devam edilir. Son ve tek kalan özetleme değerine Merkle Kökü denilmektedir. Böylelikle bir bloktan diğer bloka ulaşmada bu Merkle kökü işlevi kolaylık sağlayacaktır (Usta ve Doğantekin, 2017). Şekil 3.3'te Merkle Kök değeri hesaplanması gösterilmiştir.



Şekil 3.3. Merkle Tree Yapısı (Usta ve Doğantekin, 2017)

3.1.1.6. Zaman damgası

Her blok oluşturulurken bir zaman damgası ile oluşturulur. Bu zaman damgası geçerli zaman bilgisini tutmaktadır. Geçerli zaman bilgisi 1 Ocak 1970 tarihinden itibaren saniye olarak verir (Zheng ve ark., 2017).

3.1.1.7. Zorluk hedefi

Blokların oluşturulmasında hesaplanan özet değerleri için bazı sınırlamalar bulunmaktadır. Her bir bloğun oluşma sürecinde kullanılan ve kısıtlama koyan özel bir değerdir. Günümüzün bilgisayarları ile bir bloğun özet değerini bulmak saniyeler almaktadır. Belli bir sürede bu işlemin yapılmasını bekletebilmek için ekstra matematiksel işlemler yaptırılır. Bu matematiksel işlemlerin zorluk dereceleri bloğun başlığında yer almaktadır (Usta ve Doğantekin, 2017).

3.1.1.8. Sayaç (Nonce)

Blok oluşurken zorluk hedefi ile belirlenen şartları sağlaması gerekir. Sağlayamadığı durumda oluşan hash değeri güncellenmelidir. Blok içeriği sabit kaldığında hash değeri değişmeyecektir. Zorluk hedefinde belirlenen kısıtlamalara göre hash değeri üretilebilmesi için bloktaki diğer değerler sabit tutulurken sürekli artırılarak yeni hash değeri üretilmesine yardımcı olan “nonce” adı verilen bir değişken kullanılır. Bu değişken sayesinde bloğun başka hiçbir değişkeni güncellenmezken hash değeri nonce değişkeni sayesinde değişir (Usta ve Doğantekin, 2017).

3.1.2. Blok zincirin avantajları ve dezavantajlarının incelenmesi

Blok zinciri pek çok alanda kullanılmaktadır. Bu kullanımlar sonrasında çoğu teknoloji gibi bu teknolojinin de avantajları ve dezavantajları vardır. Blok zinciri bazen sorunlar için yeterli çözüm olmadığı gibi bazen de çözümler ihtiyacı karşılamayabilir. Bu her teknoloji için geçerli olup yapılacak işlemden önce ihtiyaçların belirlenmesi önemlidir.

Blok zinciri teknolojisi güvene ihtiyaç olmadan çalışabilen bir ortamın artırılmış güvenliği ile sunması birçok sektöre avantaj olarak yansımıştır. Bu avantajlardan en

önemlilerinden biri değiştirilemeyen veri özelliğidir. Tabi ki merkeziyetsiz yapısı gereği oluşturduğu bazı dezavantajlarda bulunmaktadır. Blok zincirinin verimliliğin merkezi olan veri tabanlarına göre sınırlı olması ve çok fazla verinin bir arada sunulmasından kaynaklı depolama kapasitesin daha fazla artmasıdır (Binance Academy, 2018).

3.1.2.1. Blok zinciri avantajları

- Dağıtık Mimari

Blok zincirinin getirmiş olduğu dağıtık mimari yapısı sayesinde ağda bulunan binlerce cihaz verileri tutmaktadır. Sistemin kendisi ve sistemde buluna veriler herhangi bir teknik arızaya ve siber saldırılara karşı dayanıklı bir yapıdadır. Ağda bulunan düğümler tüm zincirde bulunan verilerin bir kopyasını saklar. Bu sayede bir yerde oluşabilecek sorun sonucunda bir düğümün ağdan kopması ya da çevrimdışı olması ağın çalışmasını etkilemeyeceği gibi güvenlik açısından da bir problem olmaz.

- Değişmezlik İlkesi

Bloklar birbirine bağlı olduğu için onaylanan blokların geri döndürülmesi imkansıza yakın hale gelmektedir. Ağa katılan biri verileri değiştirebilmesi oldukça zordur, değiştiremediği içinde verileri manipüle edemez bunlardan kaynaklı da merkezi sistemlerde meydana gelebilecek bir veri kaybının blok zincirinde gerçekleşmesi çok güçtür.

- Şeffaflık İlkesi

Dağıtık yapısı gereği blok zincirindeki veriler tüm ağa dağıtılır. Ağda bulunan tüm katılımcılara ulaşan veriler şeffaf bir şekilde izlenebilir. Şeffaf yapısı sayesinde birçok sektörde çözümler üretilebilmektedir.

- Güvene Dayalı Olmayan Sistem

Blok zinciri yöntemi kullanılırken geleneksel ödeme yöntemleri için gerekli olan aracılar ortadan kaldırılır ve güven ortamı oluşmasa da işlemler madencilik denilen yöntem ile doğrulanabilmektedir (Binance Academy, 2018).

3.1.2.2. Blok zinciri dezavantajları

- %50+1 Saldırısı (%51 Saldırısı)

Blok zincirinde yapılabilecek saldırılar arasında yer almaktadır. Ağda bulunan tüm işlem gücünün %50'den fazlasını saldırganlar tarafından ele geçirilmesini konu alır. Bu tarz bir saldırı sonrası işlemler engellenerek maddi zararlar verilebilir ya da işlem sıralamalarının değiştirilmesi mümkün olabilir.

Bu saldırının yapılabilmesi mümkün gözükse de ağdaki katılımcı sayısı artıkça güvenlik de artar. Bitcoin blok zincirinde şimdiye kadar başarılı %50 + 1 saldırısı gerçekleşmemiştir. Bu saldırı sadece yeni oluşturulmuş işlemleri değiştirebilir. Her blok bir önceki bloğun özet değeri ile bağlı olduğu için müdahale edilebilmesi için çok yüksek bir işlem gücü gerektirir ki bu da mümkün görünmemektedir (Binance Academy, 2018).

- Özel Anahtar Erişimi

Blok zincirinde hesaplar oluşturulabilir ve bu hesapların iki anahtar değeri vardır. Biri özel anahtar diğer ise açık anahtardır. Hesap sahipleri özel anahtarlar ile kendi hesaplarına erişebilir. Eğer hesap sahibi özel anahtarını kaybederse tüm mal varlığına erişimi ortadan kalkar ve bu durum düzeltilemez.

- Depolama

Blok zinciri yapı gereği birbirine bağlı olduğundan bağlantıları koparılamaz. Bu da katılımcıların ağa dahil olduğunda ve dahil olmaya devam ettiği sürece bu verilerin tamamını indirmesi ve saklaması demektir. Ne kadar depolama büyürse ağa dahil olan düğümleri kaybetme riskiyle karşı karşıya gelinebilir. Tüm düğümler çıktığında blok zinciri çalışmaz hale gelir.

3.2. Blok Zincir Platformları

Bu bölümde blok zinciri mimarisini kullanan ve bu teknoloji ile geliştirilmiş platformlar incelenmiştir.

3.2.1. Bitcoin

Nakamoto (2008), tarafından Bitcoin sistemi ortaya atılmıştır. Bu sistem ile uçtan uca yeni bir elektronik ödeme sistemi fikri öne sürülmüştür. Kriptoloji kullanılarak Bitcoin işlemlerinin güvenliği sağlanılmaktadır. Ayrıca merkeziyetsiz yapısı sayesinde

herhangi bir şekilde bir kişi veyahut kurum bağlılığı bulunmamaktadır. Bitcoin sayesinde birçok avantaj sağlanmaktadır. Güvenlik ve anonimlik en önemli avantajlarındandır. Bitcoin ağını geleneksel sistemlerden ayıran en önemli özellikler merkezi bir sunucunun bulunmayışı ve güvenlik açısından da uçtan uca bağlı bir yapının bulunmasıdır. Bitcoin sistemi 21 milyonla sınırlandırılmış ve bu sebeple kimse bu sisteme hiçbir şekilde para ekleyememektedir. Bu sistemde blok zincir adı verilen defterlerde bu kayıtlar tutulur ve bu kayıtları tutan ve yazan kişilere madenciler denir. Bu madenciler gönüllü olarak katılır ve isterlerse üretime katılarak matematik problemlerini çözmeye devam edebilirler. Bitcoin sistemi merkezi olmayan, güvenli, şeffaf, anonim olan bir değer taşıyıcıdır (Çarkacıoğlu, 2016).

Merkezi bir otoriteye sahip olmadığı gibi Bitcoin noktadan noktaya dağıtık bir ağ olması sebebiyle de kayıtların tutulmasında güvenli olarak kabul edilmektedir. Çünkü birden fazla gönüllü ağ tarafından birbirini teyit edecek şekilde blok zincirinde kayıtlar tutulmaktadır. Bitcoin sisteminde matematiksel problemlerin çözümlenmesinde işlem gücü gerekmekte ve bunları da madencilik işlemi ile sağlanmaktadır. Gönüllülerin ödül sistemi ile de bu ağa dahil olmaları sağlanmaktadır (Gültekin ve Bulut, 2016).

Blok zinciri sistemi dağıtık veri yapısı olması sebebiyle ve merkezi bir sisteme de sahip olmadığından kullanıcıdan kullanıcıya (peer to peer) yapılan işlemlerin güvenliği otoriteden bağımsız sağlanmaktadır. Bitcoin blok zinciri sistemini kullanması sebebiyle aynı özelliklere sahip olmakta şeffaflık, güvenlik anlamında ideal bir yapı olduğu kabul edilmektedir. Üçüncü bir taraf ihtiyacına gerek duyulmaksızın katılımcıların yani madencilerin doğrulaması ile uçtan uca korunaklı bir güvenlik sistemi ile para yani değer korunmaktadır (Mendi ve Çabuk, 2018).

Bitcoin sisteminde gerçek paraya ihtiyaç duyulmaz ve bu elektronik ortamda oluşturulur. Buna da kripto para madenciliği adı verilmektedir. Bitcoin aslında herhangi bir varlığı yoktur ancak ödeme aracı olarak kullanılması sebebiyle değer kazanmaktadır. Bitcoin gerçek parada olduğu gibi, vergilendirme, banka masraf ve başkaca masrafları en düşük seviyeye getirdiği için mali yönden daha özgürlükçü olduğu söylenebilir. Blok zinciri sayesinde Bitcoin, kâğıt para gibi veyahut bankalar gibi araçlara gerek duyulmaksızın depolamayı ve aktarmayı mümkün kılar. Ayrıca madencilik denilen sistem ile de dengeli bir şekilde para üretilir ve bu para hiçbir otoriteye bağlı kılınmaz. Kripto paralarda en önemli husus gizlilik ve güvenliktir. Bitcoin yapısı bunu sağlamayı başarmaktadır (Alpago, 2018).

3.2.2. Ethereum

Vitalik Buterin tarafından 2013 yılında akıllı sözleşmeleri barındıran bir blok zincir ağı olarak ortaya çıkarılmıştır. Blok zincir teknolojisinin o güne kadar getirmiş olduğu yeniliklerden daha ileri giderek akıllı sözleşmelerin varlığı ile birçok uygulamanın geliştirilmesinin yolunu açmıştır. Bu verilerin güvenliği dağıtık ve anonim olmak üzere saklanması ve depolanmasında birden fazla sistemin kullanılması ile sağlanmaktadır. Ethereum, Ether (ETH) para birimini kullanmaktadır. Ethereum programlama dili olarak Solidity kullanmaktadır. Sözleşmelerin muhakkak kullanıcı tarafından tetiklenmesi gerekir yoksa kendiliğinden çalışmazlar. Bu sözleşmelerin çalıştırılması ve işlemlerin yerine getirilmesi için Bitcoin'den farklı olarak gas denilen bir birim vardır. Bu birim ile işlemin yapılması için ne kadar ödeme yapılacağını belirtir. Bir nevi sözleşme ücreti olarak değerini belirlemede kullanılan birim olarak da tanımlanabilir (Efendioğlu, 2020).

Ethereum, Bitcoinden farklı özelliklere sahip olsa da blok zincir tabanlı ve merkezi olmayan bir yapıya sahiptir. Ethereum'u Bitcoin ile birbirinden ayıran birçok farklılıkları vardır. Bunlardan biri doğrulama algoritması olarak farklı bir algoritma kullanılmasıdır. Ethereum'da kullanılan algoritma Ethash olarak adlandırılmaktadır. En önemli farklılık ise akıllı sözleşmeler adı verilen bir sistemin bulunmasıdır. Akıllı sözleşmeleri şu şekilde tanımlayabiliriz. Herhangi üçüncü bir kurum, kuruluş veya kişinin araya girmeksizin her türlü varlığın değişimini sağlamak amacıyla işlemler bilgisayar kodlarına dönüştürülür ve saklanır ve bu blok zincirindeki gönüllüler tarafından da denetlenir (Yavuz, 2019).

Ethereum açık kaynaklı, halka açık bir şekilde kurulan bir sistemdir. Bitcoin oluşturulurken bilgisayarın işlemcisi (CPU) kullanılırken Ethereum oluşturulurken ekran kartı işlemcisi (GPU) kullanılmaktadır. Hatta bu sayede büyük katılımcılardan ziyade ev kullanıcıları da bu ağa katılarak madencilik yapmaları mümkün hale gelmiştir. Ethereum yine merkezi olmayan bir şekilde Ethereum Sanal Makinesi olarak adlandırılan bir sisteme sahiptir. Bu sistem ile komutlar çalıştırılmakta ve gerekli depolama, hesaplama işlemleri yapılmaktadır. Ethereum, blok zinciri sisteminde yer alan otoriteden bağımsız uygulamaların kodlarını çalıştırmayı sağlamaktadır (Ata, 2019).

3.3. Blok Zinciri Mutabakat Sistemi

Mutabakat algoritmaları, dağıtık sistemlerde kullanıcılar ve makinelerin koordinasyonu sağlayan mekanizmalardır. Blok zincir ağında yeni eklenecek bloğun nasıl doğrulanacağını ve ekleneceğini planlarlar.

3.3.1. İş kanıtı (Proof of Work) (PoW)

Blok zinciri sisteminde blokların üretilmesi ve bunların blok zincirine dahil edilebilmesi için özetlemelerin doğruluğunun tespit edilmesi gerekmektedir. Ancak şifrelenmiş olan bu özetleme değerlerinin tek yönlü olduğu ve asıl veriyi tahmin etmek mümkün olmadığından, en azından bu değerlerin çözümünün doğruluğu kontrol edilebilmelidir. Kısaca tarif etmek gerekirse zincire yeni bir blok dahil edilmek istenildiğinde, çok sayıda deneme yapılarak bu işlem gerçekleştirilir. İşlem sonucunda özetleme değeri uygun olursa yeni bir blok oluşur, aksi durumda işlemler tekrarlanır ve yeni blok oluşturuluncaya kadar devam eder. Bu hesaplamalar çok fazla emek gerektirdiği için bu şekilde adlandırılmıştır (Usta ve Doğantekin, 2017).

Bu matematiksel hesaplamaları çözmeye çalışanlar madenci olarak adlandırılır. Bulunan her çözüm için sistem yeni bir para üretir ve çözümü bulan madenciye de üretilen para üzerinden ödül verilir. Bu matematiksel problem, işi talep eden kişiye göre orta zorlukta, ağ tarafında kontrol edilmesi açısından da kolay olmaktadır. Ağ da bulunan madenciler yeni eklenecek blok için oluşturulan matematiksel problemini çözebilmek için yarışırlar. Her olasılık denenerek çözümün bulunması gerekmektedir. Bu yöntem dışında başka bir yol ile çözülemediğinden dolayı çok sayıda deneme gerektirmektedir. Doğru sonucu bulan madenciye protokol tarafından para ödülü verilir ve bulunan doğru sonuç tüm ağa bildirilir. Tüm ağ yeni eklenen blok üzerinde mutabık kalarak bloğu doğrulamış olur (Gerdan, 2019).

3.3.2. Hisse kanıtı (Proof of Stake) (PoS)

PoW'a alternatif olarak çıkmıştır. PoW'a göre hedefe ulaşma süresi ve yöntemi farklıdır. Hisse Kanıtı (PoS), blok zincirde kullanıcının sahip olduğu pay ile ilişkilidir. Blok zincirinde yer alan madencilerin ellerinde bulundurdukları para miktarı ile doğru orantılı olacak şekilde yeni eklenen bloklardan ödül alır. Bu mutabakat sisteminde blok

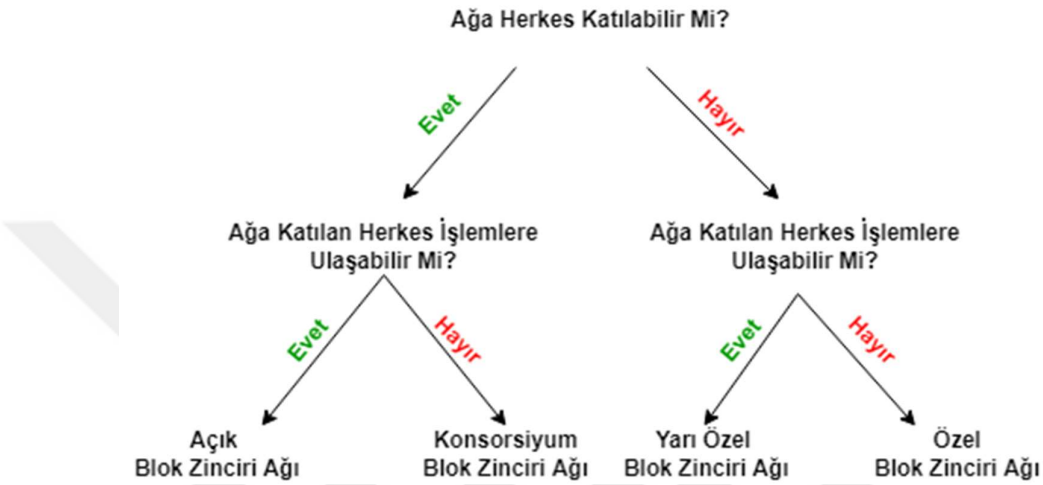
üretim sürecine madencilik değil para basma(minting) denmektedir. Bu işlemi yapabilmesi için, cüzdanında para bulunması yeterlidir. Blok zincir ağında aktif bulunan her kullanıcı tarafından otomatik olarak blok kontrolünü gerçekleştirir. Bu mutabakat sisteminde normal bir bilgisayar yeterlidir ve özel donanımlara ihtiyaç duyulmaz bu yüzdende çok yüksek bir enerji tüketimi söz konusu değildir. Sadece kullanıcının blok zincir ağında aktif olması ve blok doğrulaması yapması yeterlidir (Usta ve Doğantekin, 2017).

3.4. Blok Zinciri Ağ Türleri

Blok zincir ağları, yapıları, ödül sistemleri, şifreleme ve izin yöntemleri gibi farklı türleri mevcuttur. Bu ağların açık veya kapalı olarak tabir edilmesinde sistemin içermiş olduğu izinlerden bahsedilmektedir. Ancak farklı ağ türlerinin olması blok zincirinin temel özelliklerinin değiştiği anlamına gelmez. Yine bağımsız ve herhangi bir otoriteye bağlı kalınmaksızın verilerin değişmeyecek şekilde kaydedilmesi özellikleri tüm ağ çeşitleri için geçerli olacaktır. Açık ve kapalı olarak genel bir şekilde ağ türlerini belirlememiz mümkündür. İkisi de kendi içlerinde avantaj ve dezavantajlara sahiptirler. Açık blok zincir ağlarında kullanılan iş kanıtı algoritması ile yüksek güvenlik sağlanmaktadır. Fakat kapalı blok zincir ağlarında ise kendi içlerinde güven olduğundan iş kanıtı algoritmasının kullanılması işlem gücünün israfı anlamına gelmektedir. Bu nedenle daha az işlem gücü kullanımı için farklı algoritmalar kullanılmaktadır. Ayrıca kapalı blok zincir ağlarının merkezi otoriteden uzaklaşmaması riskinin olduğu belirtilmeli ve bu yönden açık blok zincir ağlarının kullanılması bu sorunu çözebileceği belirtilmelidir (Aghayev, 2021).

Blok zinciri yapısında verilen izne göre çeşitli ağ türleri bulunmaktadır. Açık blok zincir ağlarında herkesin blok zinciri ağına katılabilmesi mümkündür. Sistem herhangi bir otoriteye bağlı kalınmaksızın çalışmaktadır. İzin verilen sistemlerin ağa dahil olması halinde bu sisteme de özel blok zincir ağları denilmektedir. Burada blok zincirinin temel özelliğinden ayrılarak merkezi bir otoritenin ihtiyacı ön plana geçmektedir. Böylelikle bu sistemde kuralları değiştirmek ve işlemleri geri alma yetkileri bulunmaktadır. Bu durumun avantajları maliyetlerin asgariye indirilmesi ve sistemin verimliliğinin artışı olmaktadır. Konsorsiyum blok zinciri adı verilen bir sistemden de bahsedilmektedir. Bu ağ sistemi açık ve özel ağların bir arada bulunduğu sistem olarak kabul edilebilir. Açık olan bir ağda sistemdeki bazı düğümlerin yetki sahibi kişiler tarafından kontrol edilebilir

olduğu durumlarda geçerli olan bir ağ sistemidir. Böylelikle iki ağ sisteminin karakteriksel özelliklerini bir arada barındırır (Gökhan ve Uluyol, 2020). Şekil 3.4'te ağ türleri şema ile daha sade bir şekilde açıklanmıştır. Ağ üzerindeki erişim yetkilerine bakılarak hangi tip blok zincir ağ türüne sahip olduğunu söylenebilmektedir.



Şekil 3.4. Blok Zincirinde Ağ Türleri (İslam, 2019)

Otorite bulunmayan sistemler açık blok zinciri ağlarıdır. Bu sistem ile merkezi olmayan uygulamaların oluşturulması ile sunucu güvenliği sağlanmasına, altyapı oluşturulmasına ve maliyet kaygısı güdülmesine gerek kalmaz. Konsorsiyum blok zincir ağlarında ise imtiyazlı kullanıcılar bulunmaktadır. Bu imtiyazlı kullanıcılar işlemleri görebilir, isterlerse de herkesin veya belirlenen kullanıcıların görmesini mümkün hale getirebilir. Özel ağların tamamen dışa kapalı olması sebebiyle gizlilik ön plandadır. Bu sebeple de merkezi bir otoritenin olması anlamına gelmektedir ve blok zincirinin temel prensiplerine aykırıdır. Yarı özel ağda ise belirlenen koşullar veya kriterler sağlandığı takdirde erişim mümkün hale gelmektedir. İhtiyaca göre bu kullanımlar gerçekleştirilmektedir (İslam, 2019).

3.5. Blok Zincirinde Telif Hakları

Fikri hakların içeriğini insan aklının ve düşüncesinin ürettiği türler oluşturur. Fikri haklar kendi biçimleri sosyoekonomik etkiler ve bulundukları konjonktürde koruma şekillerine göre patent, ticari marka ve telif hakkı olarak ayrılmaktadır (Aghayev, 2021).

Telif haklarının korunması kapsamında ülkemizde yasal düzenlemeler mevcuttur. Bu yasal düzenlemelerin en önemlisi 5846 Sayılı Fikir ve Sanat Eserleri Kanunu (FSEK)'dur. Bu kanunun amacı "*fikir ve sanat eserlerini meydana getiren eser sahipleri ile bu eserleri icra eden veya yorumlayan icracı sanatçıların, seslerin ilk tespitini yapan fonogram yapımcıları ile filmlerin ilk tespitini gerçekleştiren yapımcıların ve radyo-televizyon kuruluşlarının ürünleri üzerindeki manevi ve mali haklarını belirlemek, korumak, bu ürünlerden yararlanma şartlarını düzenlemek, öngörülen esas ve usullere aykırı yararlanma halinde yaptırımları tespit etmektir.*", (FSEK, 1951). Telif haklarından bahsedebilmek için öncelikle bir eserin olması gerekmektedir. FSEK eser ile alakalı tanımları ve başkaca kavramların da tanımlarını yapmıştır. Kanun ile eser "*sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsulleri*" olarak tanımlanmıştır (FSEK, 1951). Ayrıca Fikir ve Sanat Eserleri Kanunu kapsamından telif haklarının geniş bir yelpazeye sahip olduğu aynı zamanda da müzik, güzel sanatlar ve sinemayı bilgisayar yazılımlarını ve bilimsel eserleri koruma altına aldığı da bu tanım ile de anlaşılmaktadır. Eser tanımlanmasında kullanılan "sahibinin hususiyetini taşıyan" tabiri, eserin sahibinin özelliklerini taşıması gerektiğini göstermektedir.

Eserin eser olma şartlarından bir diğeri ise bir maddi varlığının olması yani akıldaki fikrin dışarıya yansıtılması, aktarılması gerekliliğidir (Aghayev, 2021). Eser olması için fikrin bir ürün şeklinde herkesçe algılanabilir olması zorunludur. Dış dünyaya fikrin yansıması maddeye bürünmesi ve eserin ortaya çıkarılması ile bu eser üzerinde hak sahipliği oluşacaktır (Sert, 2008). Zaten kanun tarafından da eser sahibi eseri meydana getiren kişi olarak tanımlanmıştır (FSEK, 1951). Eserin oluşturulması ile bu eser kişiye ait olacak ve eserin fikri mülkiyet haklarına sahip olacaktır (Aghayev, 2021). Yani eserin üretilmesi ile eser sahipleri bu eserler üzerindeki hak ve yetkilerini kullanacaktır (Sert, 2008).

İnternetin varlığı ile aslında eserlerin iletilmesi daha da kolay hale gelmiş, ancak bu durum telif hakları sorunlarına yol açmıştır (Sert, 2008). Dijitalleşen dünyada fikri ürünlerin herkes tarafından kolayca üretilebilmesi ile sunulan telif hakkı koruması kapsamında eserlerin kopyalanıp dağıtılması da bir sorun haline gelmiştir. Aynı zamanda da fikri ürünlerin üretiminin engellenemediği yani dijital mecralarda taklit edilmesi, kopyalanmaların kolay olmaları ve fikri emeklerin bu tür mecralarda paylaşılmasının önüne geçilememektedir. Dijital olarak oluşturulan bu eserler sınırsızdır. Sınırsız olmaları değersiz oldukları anlamına gelmemektedir. Aksine çok fazla fikri çaba ve yine ekonomik

destekler ile bu eserler meydana gelmektedir. İnternetin hızlı ve erişilebilirliğinin fazla olması nedeniyle fikri ürünlerin bu ortamının sağladığı gizlilik ile farklı mecralarda kendilerine aitmiş gibi fikri ürünün paylaşımının yapılması yolunu açmıştır. Burada ise telif hakları eser sahibini koruma amaçlı olarak devreye girecektir (Aghayev, 2021).

Telif haklarının en büyük sorunlarından biri sınırsız olan fikri ürünlerin sahibinin kim olduğu ve bu bilginin doğrulanabilirliğidir. İşte burada da özelliklerinden bahsetmiş olduğumuz blok zincirinden faydalanabilir. Blok zincirinin değiştirilemeyen kayıt özelliği ile birçok konuda telif haklarını koruma ve eserin aidiyetinin belirlenmesi sağlanabilir. Blok zincir üzerinde eserin kimin tarafından üretilmiş olduğu değiştirilemez bir veri yapısıyla kayıt altına alınmaktadır. Böylelikle aidiyet bilgilerinin içeriği koruma altına alınmaktadır (Şenkardeş, 2021). Blok zinciri yapılarının özelliği olan dağıtık yapı sayesinde eski sistemlerdeki saklanan veriler sadece tek merkezde toplanmamakta ve böylece tek merkezcilikten doğan sorunlar aşılmaktadır. Bunun sebebi kayıtlar değiştirilemez, manipüle edilemez ve veri kaybı oluşturulamaz olmasıdır (Aghayev, 2021).

Telif hakları yukarıda belirttiğimiz gibi eserin oluşturulması ile doğmaktadırlar. Bu nedenle eserin ne zaman üretilmiş olduğunun da öneminin olduğu ortadadır. Yine blok zincirinin değiştirilemezlik özelliğinin yanı sıra zaman damgası özelliği de bu noktadan önem kazanacaktır. Zaman damgası eserinde daha önce üretilip üretilmediğini ya da ilk olarak kim tarafından üretildiğini belirleyecek niteliktedir. Telif hakları, üretim ve aidiyetlik bilgileri kayıt altına alınırken, blok zincirinin zaman damgalı koruması sayesinde sistemin güvenliği ve ispatı sağlanmaktadır (Şenkardeş, 2021). Zaman damgası ile gerçekleştirilen onaylama eserin ortaya konduğu zamanı değiştirilemez kılacaktır. Eser sahibinin de onay zamanına müdahale edemiyor olması da sistemin güvenli olmasını sağlamaktadır (Aghayev, 2021).

Blok zincir uygulamalarıyla dijital fikri eserlerin, zaman damgası ile kayıt altına alınması ve aynı zamanda da bu bilginin orijinalliği doğrulanabilmektedir (Şenkardeş, 2021). Aslında bu sayede eser sahibine eserine zaman damgası oluşturmasını ve bu eserinin aidiyetini gösteren telif hakkını ispatlar nitelikte sertifikalar verilebilir (Babaoğlu ve Karasoy, 2022). Telif hakkının belgelendirilmesi amacıyla kullanımı halinde resmi otoritelerin kabulü ile kullanılabilir olabilir. Blok zincirinin telif haklarındaki yansıması eser sahibi ve orijinalliğin belirlenmesi için bu hakların belgelendirilmesi mümkün hale gelebilmektedir. Blok zinciri bu sayede fikri ürünlerin yani fikri eserlerin sahipliğinin

belirlenmesi, korunması gibi durumlarda etkili bir çözüm olarak değerlendirilebilir (Demir, 2019).

3.6. Akıllı Sözleşmeler

Akıllı sözleşmeler, blok zincirinde depolanan kod parçacıklarıdır. Bu kod parçacıkları blok zinciri üzerinde verilerle işlem yapabilen uygulamalardır. Gerçek sözleşmeler ile bağlantılı olmasalar da bu programlar kodlanırken belirlenen koşullara göre sözleşmeye katılan hesaplar üzerinde işletilir. Akıllı sözleşmeler blok zincirine gönderildiğinde, blok zinciri üzerindeki hesaplar gibi bir adres değerine sahip olur. Gönderildikten sonra bu akıllı sözleşmeler değiştirilemez. Güncelleme yapılmak istendiğinde yeni versiyonu yazılır ve tekrardan blok zincirine gönderilir. Bu işlem sonucu yeni hesap açılmış gibi akıllı sözleşmenin yeni adres değeri oluşturulur. Akıllı sözleşmenin koşulları neler ise koşullar sağlandığında blok zincirinde bulunan düğümler tarafından otomatik çalıştırılır ve sözleşmede belirlenen işlemler gerçekleşir (Buterin, 2014).

3.7. Hardhat Geliştirme Ortamı

Bir geliştirme ortamı olan HardHat, Ethereum blok zincir ağı için geliştirilmiştir. Akıllı sözleşmeleri derleme işlemini, bir akıllı sözleşmeyi blok zinciri üzerinde dağıtıp yayına almak, bu yayına alma işlemi öncesinde birçok kez test edebilmek ve hataları ayıklayıp sorunları çözebilmek için gerekli ortamı sunmaktadır. Akıllı sözleşmeler ve merkeziyetsiz uygulamalar oluşturma sürecini hızlandırdığı gibi yönetilmesini kolaylaştırmaktadır (Usta, 2022).

3.8. Şifreleme Yöntemleri

Verilerin güvenliğinin sağlanabilmesi için kriptolojik yöntemlerden geçirilerek şifreli bir değer üretilmesi gerekmektedir. Bu kısımda şifreleme yöntemlerinden bahsedilecektir.

3.8.1. Kriptolojik özet fonksiyonu

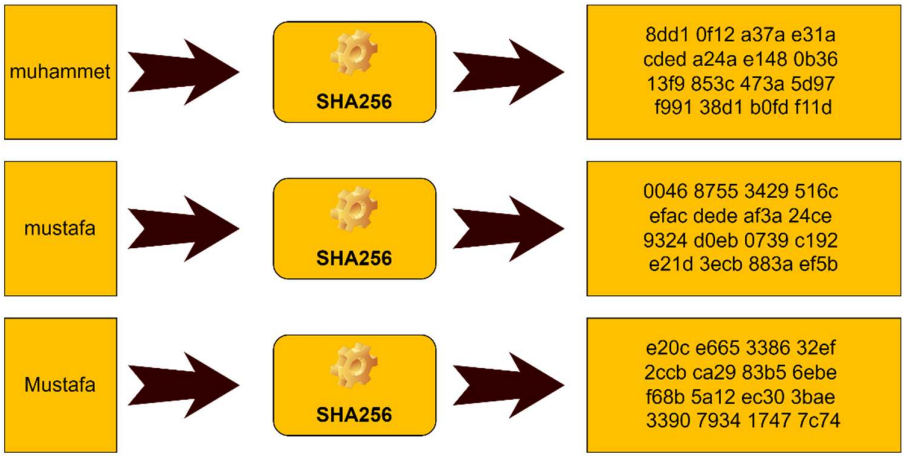
Bir veri topluluğunun yani dijital bilginin girdi olarak alınarak kendisinden daha küçük bir özet bilgiye dönüştürülme işlemini özetleme (hash) kavramı olarak tanımlanabilir. Güvenli kavramı ile bu işlemin yapılırken şifreli bir şekilde yapılması amaçlanmış olduğu görülmektedir. Güvenli özetleme (secure hash) dijital verinin şifrelenmesi suretiyle özet bir bilgi oluşturulmasıdır denilebilir. Burada farklı verilerin farklı özet bilgileri vermesi beklenir. Tek bir verinin değişikliği halinde bile özet bilgilerde değişiklik olacaktır. Aynı zamanda da bu işlem güvenli olması tek yönlü olmasını gerektirir ki tek yönlü olma özet bilgiye dönüşen verinin, özet bilgi ile elde edilemeyeceği anlamındadır. Yani özet bilgi geriye döndürülemez biçimde bulunur. Bu özet bilgiden başka bir bilgi üretimi de mümkün değildir. Özet bilginin ancak önceki verinin özetlenmesi ile doğruluğu bulunabilir. Farklı algoritmalar olmasına rağmen blok zincirinin daha güvenli hale gelmesini sağlayan SHA256 hash algoritması önemli algoritmalardan biridir. Güvenli özetleme algoritmaları eldeki uzun veya kısa veriyi her zaman 256 bitlik özet yapıya çevirmektedir. Bu özetlemenin güvenlik amacıyla şifrelenmesi nedeniyle geriye döndürülmesi mümkün değildir ve önceden tahmin edilemez, bu nedenle mesaj özetinin 256 bit yaklaşık 2^{256} farklı kombinasyon olacağından tahmin edilmesi uzun zaman alacaktır. (Usta ve Doğantekin, 2017).

Şekil 3.5'te SHA256 kriptolojik özet fonksiyonun çalışma yapısını gösterilmiştir. Gelen girdi dosya alınır ve SHA256 hash algoritması tarafından bir değer üretilir. Bu değer geri döndürülerek orijinal dosyayı tekrar üretmek mümkün değildir.

Şekil 3.5. SHA256 Çalışma Yapısı

İçeriği değiştirilmemiş aynı dosya farklı zamanlarda bu algoritma ile kullanılsa bile aynı değeri üretecektir. Bu algoritma dosya veya verilen bir kelime ya da cümle üzerindeki tüm değişiklikleri hatta her harfi veya küçük büyük harf duyarlılığını tespit

edip farklı bir değer üretmektedir. Bu algoritmanın örnek çıktılarının göstermek için Şekil 3.6'da bir örnek gösterilmiştir. Bu örnek SHA256 hash algoritmasına tabi tutulan kelimelerin ürettiği sonucu göstermektedir.



Şekil 3.6. Hash Algoritması Örnek Girdi ve Çıktılar

3.8.2. Sayısal imza

Belgelerde imzaların bulunması, belgenin imzayı atan kişi ya da kişiler tarafımızdan yapıldığını kanıtlar. Dijital içeriklerde sayısal imza mevcuttur. Sayısal imza belgenin içeriğine göre değişmektedir. Sayısal imzanın getirdiği tanıma, veri doğrulama, inkâr edilememe gibi özellikleri vardır.

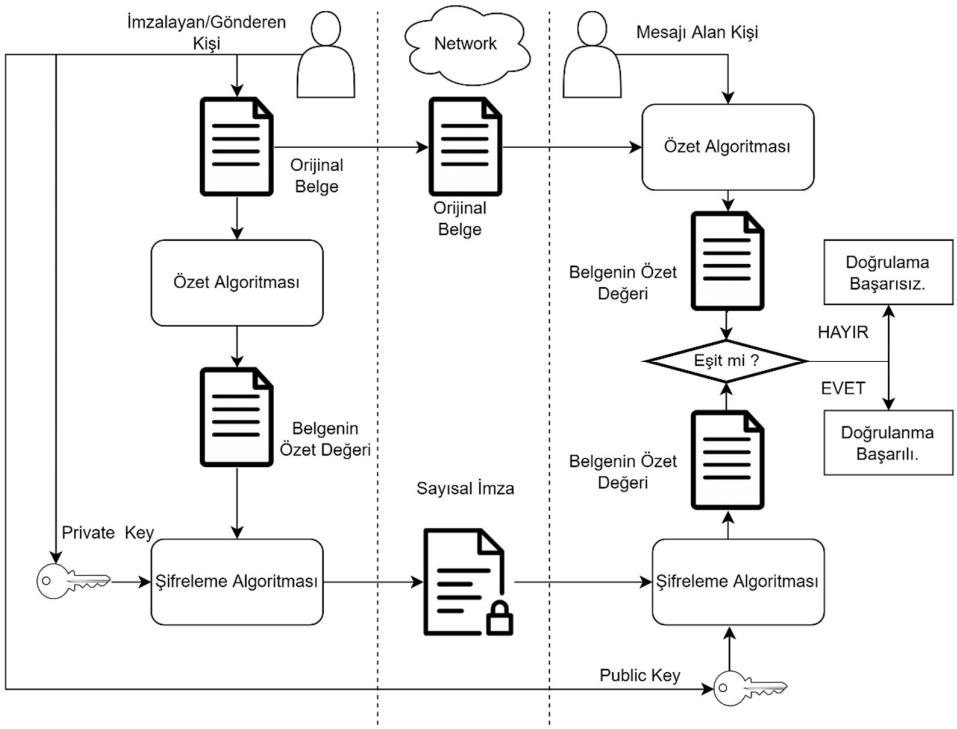
Sayısal imza ile gelen tanıma, bir kişinin kimliğinin onaylanma işlemidir. Belgeyi imzalayan kişinin kimliğini tespit ederken, bir başkası tarafından gönderilen bilginin değiştirilemediğini ispatlanması için kullanılır (Kodaz ve Botsalı, 2010).

İmzalanan belgenin doğruluğu sayısal imza vasıtasıyla onaylanır. Sayısal imza ayrıca oluşturulan belgenin değiştirilmediğini ispatlayan bir yöntemdir. Sayısal imza, imzalanmış belgenin sayısal özet değerini içerir. Orijinal belgede yapılacak en ufak bir değişiklik sonucu belgenin sayısal özet değeri değişeceğinden sayısal imzanın geçerliliği doğrulanamaz. Bu şekilde imzalanan belgenin gönderen kişi tarafından imzalanıp imzalanmadığı bilinebilmektedir.

İmzalayan kişinin kimliği tespit edilebilmektedir. İmzalama aşamasının daha sonrasında o belgeye kimlerin katıldığını bulabilmemize olanak tanır. Gönderici belgenin

imzaladığını inkâr edemediği için yazılı belgelerdeki imzalar gibi burada da bir bağlayıcılık bulunur.

Şekil 3.7'de gösterilen orijinal belge, özet fonksiyonu olarak belirtilen SHA256 hash fonksiyonu ile etkileşime girerek bir özet değeri üretilir. Üretilen bu değer geri döndürülemez tek yönlü bir işlemdir. Bu değer kullanılarak da orijinal dosya üretimi de yapılamaz. Orijinal dosya kullanılması gereklidir ve içeriği değişen bir dosyanın özet değeri farklı olacaktır. Herhangi bir değişiklik olması durumunda imza geçersiz olur.



Şekil 3.7. Sayısal imza ile imzalanan belgenin iletilmesi ve doğrulanması

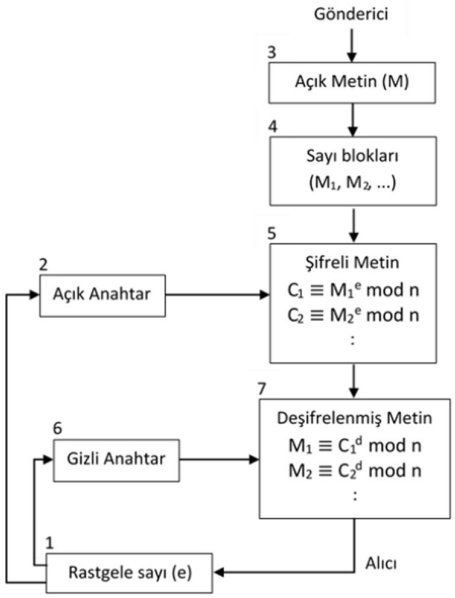
Orijinal belgenin özet değeri üretildikten sonra imzalayan ya da gönderen kişi tarafından kendisine ait özel anahtarı (private key) ile şifrelenir ve alıcıya gönderilir. Alıcı bu belgenin gönderen kişiye ait olduğunu ispatlayabilmek için orijinal belge ve sayısal imzaya ihtiyacı vardır. Orijinal belgenin özet değerini hesaplar. İmzalanan belgeyi de gönderen kişinin genel anahtarı (public key) ile çözerek gönderen kişinin imzaladığı özet değerini elde eder. İki özet değerini karşılaştırarak eşit olup olmadığına bakar. Eşit ise imzalanan belgenin doğruluğunu kanıtlar aksi takdirde imzanın doğruluğu başarısızdır.

3.8.3. RSA yöntemi

RSA algoritması hem şifreleme hemde sayısal imza atabilme olanağı tanıyan açık anahtar kullanan bir yapıdır, (Kodaz ve Botsalı, 2010). Bu şifreleme algoritması 1977'de Ron Rivest, Adi Shamir ve Lonard Adleman tarafından geliştirilmiştir. Algoritma geliştiren kişilerin soy isimlerinin baş harfleri kullanılarak isimlendirilmiştir. Açık anahtar şifrelemede kullanılan bir algoritmadır. Çok büyük değerlikte iki asal sayının çarpımı sonucu oluşan bir tam sayı değeri verildiğinde bu sayının çarpanlarına ayrılması zordur, (Akben ve Subaşı, 2005). İki asal sayının çarpımı sonucunda bir temel değer üretilir. Diğer anahtarlarda bu iki asal sayı ile üretilir. Bu nedenle anahtar boyutu artırırsak şifreleme gücüde artacaktır, (Bote, 2021). RSA yöntemi bu matematiksel işleme dayanır.

RSA iki farklı anahtar şeklinde çalışır. Açık anahtar (public key) ve gizli anahtar (private key) üzere iki anahtar vardır. Açık anahtar herkese verilir ve gizli anahtar kişiye özeldir ve gizli tutulur. Açık anahtar ile özel anahtar arasında matematiksel bağ vardır ve genel anahtar ile özel anahtara ulaşmak mümkün değildir. Bir metni şifreleyip göndermek isteyen bir kullanıcı bu açık anahtarı kullanır ve metni şifreler. Şifreli metnin çözülebilmesi gizli anahtara bağlıdır. Gizli anahtar ile şifreli metin çözülebilmektedir, (Beşkirli ve ark., 2019).

Şekil 3.8'de RSA algoritmasının gönderici ve alıcı arasındaki akışın şeması verilmiştir.



Şekil 3.8: RSA Algoritmasının Akış Şeması (Beşkirli ve ark., 2019)

RSA algoritmasının anahtar oluşturma adımları aşağıdaki gibidir.

1. Büyük değerlikte birbirinden bağımsız iki adet asal sayı seçilir. Bu sayılar ne kadar büyük olursa güvenlik açısından o kadar iyidir. Bu asal sayılar p ve q olsun.
2. Anahtarlar için temel bir değer hesaplanması gerekmektedir. Temel değer için n harfini kullanılırsa; Denklem 3.1'deki gibi hesaplanır. Bulunan n değeri için totient fonksiyonundaki değeri Denklem 3.2'deki gibi hesaplanır.

$$n = p * q \tag{3.1}$$

$$\varphi\,(n) = (p-1) * (q-1) \tag{3.2}$$

3. $1 < e < \varphi\,(n)$ aralığında bulunan ve Denklem 3.3'teki eşitliği sağlamak üzere rastgele bir e sayısı üretilir ve e sayısı açık anahtar olarak kullanılır.

$$ebob(\varphi\,(n),\ e) = 1 \tag{3.3}$$

4. $1 < d < \varphi\,(n)$ aralığında bulunan ve Denklem 3.4'te olmak üzere bir d sayısı üretilir ve d sayısı gizli anahtar olarak kullanılır.

$$(e * d) mod\ \varphi\,(n) = 1 \tag{3.4}$$

3.8.3.1. Şifreleme

Şifreleme aşamasında genel anahtar ve temel değerler kullanılır. (e, n) ikilisi Denklem 3.5'te gösterilen matematiksel işlem kullanılarak şifreleme yapılır.

$$C \equiv M^e (mod\ n) \tag{3.5}$$

Denklem 3.5'te sağlayan matematiksel işlem de e genel anahtar olarak kullanılır. Gönderilecek mesaj M [0, n-1] arasında bulunacak şekilde tam sayıya çevrilir. Elde edilen C değeri ise şifrelenmiş metindir. Alıcıya bu C değeri (şifreli mesaj) gönderilir.

3.8.3.2. Şifre çözme

Bilgiyi alan kişi gizli anahtarını kullanır. Denklem 3.6'te eşitliğini sağladığında açık metin elde edilmiş olur. Bu şekilde mesaj ve gönderen kişi doğrulanır.

$$M \equiv C^d (mod\ n) \tag{3.6}$$

3.8.4. X.509 açık anahtarlama altyapısı

X.509, ortak anahtar sertifikalarının yapısı ve hiyerarşik formatını tanımlayan bir standarttır (Varma, 2020). X.509 sertifikaları güvenli protokol olan HTTPS'nin temelini oluşturan TLS/SSL dahil olmak üzere birçok internet protokolünde kullanılmaktadır. Ayrıca dijital imzalar gibi çevrimdışı uygulamalarda da kullanılmaktadır. Bir açık anahtar veya bir kimlik içerir ve bir sertifika veren kuruluş yada yetkili tarafından imzalanabildiği gibi bireyin kendisi de imzalayabilir (Vikipedi, 2022). Bir sertifikada bulunan ortak anahtarlar kullanmadan önce, ilk olarak bu sertifikanın gerçekliğini ve özellikle ortak anahtar oluşturulması için gerekli tüm sertifikaların geçerliliğinin belirlenmesi gerekir (Cooper ve ark., 2005). Bu sayede başka biri tarafından açık anahtarlara güvenilebilir.

Bu sayede dijital sertifikalar ile bir kimliği şifreleyebilir, oturum açma işlemleri veya dijital bilgilerin şifresini çözmek için kullanılabilir. Bu işlemleri yaparken bir çift dijital anahtar kullanılır. Açık anahtar, bir dizi rastgele sayıdan oluşmaktadır ve bir mesajı şifrelerken kullanılabilir. Bu şifrelenen mesajı çözebilme kabiliyeti yalnızca alıcıya aittir. Şifreli mesajı çözümleyebilir, okuyabilir bunu yapabilmesi için açık anahtar gibi bir dizi rastgele sayıdan üretilen ve matematiksel olarak birbiri ile ilişkili özel anahtar kullanılmalıdır. Bu özel anahtar gizlidir ve sadece alıcı tarafından bilinir. Açık Anahtar, herkese açıktır ve kaba kuvvet algoritmaları (brute force attack) ile istismar edilemeyecek şekilde değişken ve uzun rastgele sayısal kombinasyonlar üreterek bunları özel anahtarla eşleştirmek için karmaşık bir şifreleme algoritması kullanılarak oluşturulur (Sectigo, 2021).

Genel anahtarların boyutu veya bit uzunluğu, korumanın ne kadar güvenli olacağını belirler. Örneğin; 2048 bit RSA anahtarları genellikle SSL sertifikalarında, dijital imzalarda ve diğer dijital sertifikalarda kullanılır. Bu anahtar uzunluğu algoritmanın kırılmasını önlemek için yeterli şifreleme güvenliği sağlamaktadır (Sectigo, 2021).

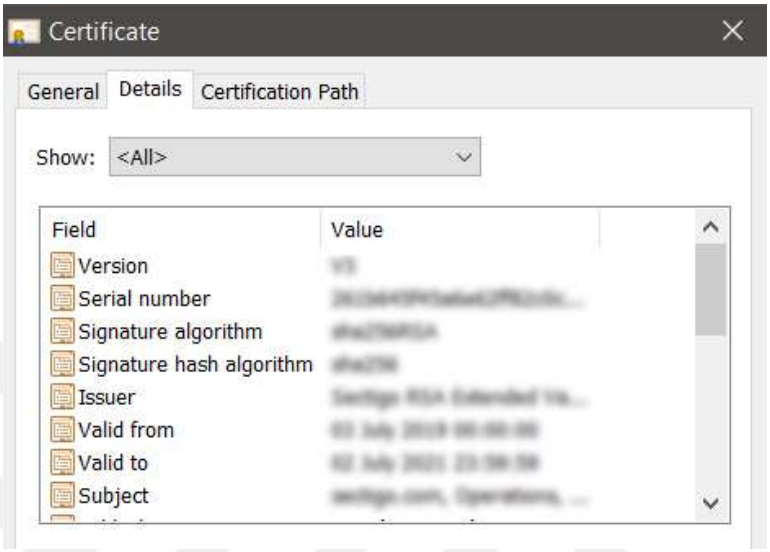
Şekil 3.9'de görüleceği üzere açık anahtar şifreleme işlemi yaparken gizli anahtar ile bu şifreler çözülebilecektir. Gizli anahtar ile dijital olarak belgeler imzalanabilirken açık anahtar ile bu imzanın doğruluğu kanıtlanabilir. Gizli anahtarlar ayrıca kimlik bilgisini oluşturmada kullanılır. Açık anahtar ile kimlik bilgilerinin doğruluğu ispat edilebilir (Sectigo, 2021).

Şekil 3.9. X.509 sertifikalarını kimlik doğrulama ve güvenlik için özel anahtarların kullanımı (Sectigo, 2021)

Şekil 3.10'da gösterilen X.509 sertifikasında bulunan temel özellikler şu şekilde özetlenebilir (Hasırcıoğlu ve Öz, 2008) ;

- Sürüm: X.509 standardında oluşturulan sertifikanın eklentilerine göre v1, v2, v3 olarak tanımlanan sürümlerini belirtir.
- Sertifika Seri Numarası: Sertifikayı üreten hizmet sağlayıcı tarafından sertifikayı diğerlerinden ayıran benzersiz seri numarası tanımlayıcısıdır. Yayınlayan adı ve sertifika seri numaraları tek bir sertifikaya özgüdür.
- İmzalama Algoritması: Sertifika hizmet sağlayıcı tarafından sertifikayı imzalamak için kullanılan imzalama algoritmasını tanımlayan özelliktir. Bu algoritmanın açık anahtar alanında bulunan algoritma ile eşleşmesi gerekmektedir.
- Sertifikayı Yayınlayan: Sertifikayı imzalayan ve yayınlayan kuruluşa ait bilgileri içermektedir.
- Geçerlilik Periyodu: Sertifikanın geçerli olacağı başlangıç ve bitiş tarih aralığını saat bilgisi dahil göstermektedir.
- Konu: Sertifika hizmeti sağlayan kuruluş tarafından verilmekte olan kullanıcıyı, bilgisayar adını, hizmeti veya ağ aygıtını belirtmektedir.
- Açık Anahtar: Sertifika ile ilişkilendirilmiş anahtar çiftlerindeki açık anahtarı gösterir.

- Sertifikasyon Merkezi İmzası – Parmak İzi: Sertifikasyon merkezi tarafından imzalanan dijital sertifikanın içerik özetini gösterir.



Şekil 3.10. Standart bir sertifika parametreleri (Sectigo, 2021)

3.8.5. Eliptik eğri dijital imza algoritması (ECDSA)

Eliptik eğri kriptografisi (ECC) Neal Koblitz ve Victor Miller tarafından 1985 yılında bulunmuştur. Eliptik eğriler kriptografiğinin güvenliği için ayrık logaritma problemlerine dayandırılmıştır (Johnson ve ark., 2001). Eliptik eğri dijital imzalama algoritması (ECDSA), sayısal imzalama algoritması olarak kullanılabilir.

Denklem 3.7'da k değeri ve eliptik eğri üzerinden P noktası verildiğinde Q noktası Denklem 3.7'da yerine koyarak daha kolay hesaplanabilirken sadece Q ve P noktaları verildiğinde ayrık logaritma problemi sebebiyle k değerini hesaplayabilmek gerçekten zordur (Sarıtaş, 2010).

$$Q = kP \quad P, Q \in EF(a, b)\ ,\ k < p \tag{3.7}$$

En büyük kripto para birimlerinden biri olan Bitcoin'de işlem yapılabilmesi için kullanıcı kendi özel anahtarı ile yapılacak işlemi imzalaması gerekir. Bu imzalama işlemi ECDSA ile gerçekleşmektedir. Bu tarz platformlarda ECDSA algoritmasını kullanılma sebebi, RSA algoritmasına göre daha düşük anahtar uzunluğunda daha fazla güvenlik sağlamasıdır (Oğuzhan ve Kiani, 2018).

ECDSA algoritmasına ait domain parametreleri ve aşamaları (Johnson ve ark., 2001);

- Parametreler
    1. Bir sonlu cismin boyutuna q, bir p asal sayısına eşit veya m pozitif tam sayısı ile Denklem 3.8'deki gibi ifade edilir.

$$q = 2^m \tag{3.8}$$

    2. F_q da bulunan a ve b iki alan elemanı E olarak tanımlanır. F_q bir eliptik eğri ve bunun üzerinde Denklem 3.8 ve 3.9'da kullanılarak ifade edilir.

$$y^2 = x^3 + ax + b \quad , p > 3 \tag{3.9}$$
$$y^2 + xy = x^3 + ax^2 + b \quad , p = 2 \tag{3.10}$$

    3. $E(F_q)$'da asal sayı olarak bir G = (x_g, y_g) sonlu noktası tanımlanır. Eliptik eğrisinin noktalarının oluşturan grup için bir üreteci $P = (x_p, y_p)$ şeklinde belirtilir.
    4. Bu sonlu noktanın mertebesi n ile ifade edilir, Denklem 3.11'deki eşitsizliğini sağlar ve eş çarpan değeri Denklem 3.12'de verilmiştir.

$$n = 4\sqrt{q} \quad , n > 2^{160} \tag{3.11}$$
$$h = E(F_q)/n \tag{3.12}$$

- ECDSA kullanılarak bir A katılımcısı için anahtar çiftini oluşturma;
    1. Bir d tam sayısı [1, (n-1)] değer aralığında bulunacak şekilde rastgele seçilir.
    2. Denklem 3.13 ve 3.14 hesaplanarak A katılımcısının anahtar çifti (pk, sk) oluşturulmuş olur. A katılımcısı için açık anahtar pk; Gizli anahtar ise sk olarak tanımlanmıştır.

$$pk \leftarrow d * G \tag{3.13}$$
$$sk = d * G \tag{3.14}$$

- ECDSA kullanılarak, A katılımcısı bir *m* mesajını bahsedilen domain parametreleri ve anahtar çifti (*pk, sk*) ile kullanarak imza oluşturma aşaması;
    1. $1 \leq k \leq n$-1 aralığında şifreleme için güvenli bir k tam sayısı rastgele olarak seçilir.
    2. Eliptik eğri noktası Denklem 3.15'te gösterildiği gibi hesaplanır. Elde edilen değer x_1 değeri bir tam sayıya çevrilir.

$$(x_1, y_1) \leftarrow kG \tag{3.15}$$

    3. Denklem 3.16'nın hesaplaması sonucunda, eğer *r* değeri 0 ise 1.adıma dönülerek tekrar başlanır.

$$r \leftarrow (x_1 mod\ n) \tag{3.16}$$

    4. *m* mesajı *H* özet fonksiyonu kullanılarak *H*(*m*) değeri bulunur ve elde edilen bit dizisi e ile gösterilen bir tam sayıya çevrilir.
    5. Denklem 3.17 hesaplanır. Hesaplanan *s* değeri 0 ise 1.adıma geri dönülerek tekrar başlanır.

$$s \leftarrow k^{-1}\,(e + sk * r)\ mod\ n \tag{3.17}$$

    6. Son olarak A katılımcısının m mesajı için oluşturulan imza Denklem 3.18'de gösterildiği gibi ifade edilir.

$$\sigma = (r, s) \tag{3.18}$$

- ECDSA kullanımında A katılımcısının domain parametreleri ve A katılımcısının *pk* (açık anahtar) değeri B katılımcısına gönderilir. *m* mesajı için A katılımcısının oluşturduğu imzanın doğrulaması yapılmadan önce B katılımcısı domain parametrelerinin de doğrulmasını yapabilmektedir. İmza doğrulama algoritmasının aşamaları;

1. *r* ve *s* tam sayı değerlerinin [1, (*n*-1)] aralığında olup olmadığı kontrol edilir.
2. *H*(*m*) değeri bulunur ve elde edilen bit dizisi bir tam sayıya (*e*) çevrilir.
3. Denklem 3.19 hesaplanır.

$$w \leftarrow (s^{-1}\ mod\ n) \tag{3.19}$$

4. Denklem 3.20 ve Denklem 3.21 hesaplanır.

$$u_1 \leftarrow (e * w\ mod\ n) \tag{3.20}$$
$$u_2 \leftarrow (r * w\ mod\ n) \tag{3.21}$$

5. Denklem 3.22'de *X* değeri hesaplaması yapılarak bir eğri noktası elde edilir, eğer *X* değeri 0 ise imza doğrulaması başarısızdır. Başarılı ise *X*'in x koordinatı x_1 ile ifade edilir.

$$X \leftarrow (u_1 * G + u_2 * pk) \tag{3.22}$$

6. Denklem 3.23'de yer alan *v* değeri hesaplanır. Eğer *v* değeri *r değerine eşit* ise imza doğrulaması başarılı bir şekilde yapılmış olur.

$$v \leftarrow (x_1\ mod\ n) \tag{3.23}$$

3.8.5.1. Eliptik eğri şifreleme güvenliği ve performansı

Eliptik Eğri Kriptolojisinin (ECC) güvenliği yüksek düzeyde sağlarken imzalama ve doğrulama performansının da yüksek olması gerekmektedir. Yapılan bir çalışmada ECDSA için tekil imzalama işlem süresi ortalama olarak **0.534 milisaniye** olarak hesaplanmıştır. Aynı şekilde doğrulama işlemi içinde ölçümleme yapılarak tekli imzada doğrulama işlemi **0.463 milisaniye** hesaplanmıştır (Akyüz, 2021).

ECC güvenliği, eliptik eğri logaritması problemine dayanır. Sayısal imza algoritması veya RSA yöntemindeki sayısal imzadalar da sağlanan güvenlik düzeyine ulaşabilmek için N sayısı yaklaşık olarak 160 bit olmalıdır. Böylelikle eliptik eğri imzası daha küçük bir sonlu cisimde işlem yapar ve aynı güvenliği sağlar (Sarıtaş, 2010).

Bu çalışmada akıllı sözleşmenin tarafından girdiler işlenmektedir. İşlenen girdilerin ürettiği çıktılar ile kanıt dosyası oluşturulmaktadır. Kanıt dosyası üretilebilmesi için hızlı ve güvenliğinin yüksek olduğu bir şifreleme yöntemi olan ECDSA algoritması tercih edilmiştir.

3.8.6. JSON Web Token (JWT)

JSON Web Token (JWT), iki taraf arasındaki iletişim için bir JSON nesnesi olarak bilgi gönderimi için tasarlanmış güvenli bir yapıdır (Jones ve ark., 2015). JWT ile taşınan bilgiler, dijital olarak imzalanabilir olduğundan mesaj doğrulanabilir ve güvenilir olmaktadır. JWT yapısı, gizli hash tabanlı mesaj doğrulama kodu (Hash-Based Message Authentication Code – HMAC), RSA yada ECDSA algoritmaları kullanılarak genel ve özel anahtar çiftleri ile imzalanabilir (Peyrott, 2016).

JWT sistem kimlik doğrulamalarında kullanılır ve bilgi alışverişlerinde kullanılan JSON dizesi kendi kendine yeten bilgi biçiminde bir belirteçtir. JWT'ler küçük boyutlu olması sebebiyle URL'ler ve HTTP POST parametrelerinde veya HTTP protokollerinin başlıkları üzerinden gönderilebilir ve bu nedenle de daha hızlıdır (Rahmatulloh ve ark., 2018).

JWT, JSON yapısı kullandığı için diğer alternatif yapılara göre kompakt bir yapıdadır. Alternatiflerinde kullanılan XML yapısına göre, HTTP protokolünde JWT'yi transfer etmek daha kolay gerçekleşir. Çoğu programlama dilinde JSON'a özel ayrıştırıcı fonksiyonları bulunur. Geliştiriciler, bu açıdan kolay ayrılabilen JSON verilerini tercih etmektedir.

3.8.6.1. JWT yapısı

Bir JWT yapısını oluşturan üç bölüm vardır. Bu kısımlarda JSON nesneleri Base64 ile kodlanarak oluşur ve birbirlerine nokta (.) ile bağlıdır. Örnek bir JWT yapısı Şekil 3.11'de gösterilmiştir.

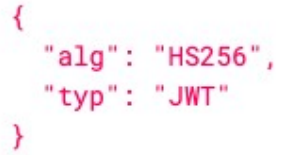
Şekil 3.11. Örnek JWT Yapısı: Kırmızı (Header).Mor (Payload).Mavi (Signature)

Şekil 3.11'da gözüktüğü gibi üç parçadan oluşan bu yapının ilk kısmı header, ortada kalan kısım payload ve son kısımda signature bölümünü oluşturmaktadır. Kısaca bölümleri şu şekilde tanımlayabiliriz;

Header (Başlık)

Bu alanda bulanan iki bölüm vardır. Biri belirteç türünü belli eder diğeri ise JWT'nin imza bölümünde kullanılan karma algoritmayı temsil eder. Belirteç türü olarak JWT, karma algoritma türü olarak da HMAC, SHA256 veya RSA gibi kullanılan karma algoritmalar yazılabilir.

Şekil 3.12'de başlık bölümünde yer alan bilginin kodu çözülmüş hali yer verilmiştir. Burada alg alanında yazan HS256 algoritması, imzayı oluşturulabilmesi için kullanılacak olan HMAC ve SHA256 algoritmalarının beraber kullanımını temsil eder. Bu alan JWT oluşturulurken Base64 ile kodlanarak kullanılacaktır.



Şekil 3.12. Başlık Bilgisinin Kodunun Çözülmüş Hali

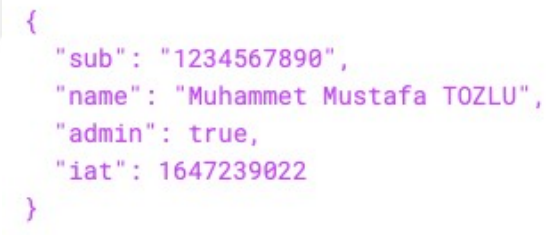
Payload (Veri)

Transfer edilecek bir varlığın claim adı verilen bilgilerini içerir. Claim o varlığın hakkında ileri sürülen bilgi parçalarıdır. Buradaki kullanımı, transfer edilecek varlığın hakkında bilgiler vermesi ve JWT yapısının doğrulama aşamasında bu bilgilere bakılarak bazı işlemlere izin verilmesi sağlar.

Üç çeşit claim türü mevcuttur. Bunlar; registered (kaydedilmiş), public (genel), private (gizli) claim'lerdir.

- **Registered Claims:** JWT yapısına önceden eklenmiş claim türleri bulunmaktadır. Bu claimlerin kullanımı zorunlu olmasa bile kullanıldığında yararlı olacak bilgileri barındırır. Bu alan içerisinde iss(issuer), exp(expiration time), sub(subject), aud(audience) gibi claimler örnek verilebilir.
- **Public Claims:** JWT yapısında isteğe göre eklenen alanlardır. Fakat registered(kaydedilmiş) alanında veya URI'de tanımlanan özellikler ile aynı olmaması gerekir.
- **Private Claims:** Mevcut claimler dışında kullanılabilen özel bilgileri bu alanda yer alır.

Şekil 3.13'te örnek payload(veri) bilgisi verilmiştir. Bu alan JWT kullanımında base64 ile kodlanarak kullanılır. Dikkat edilmesi gereken durum ise JWT bu kısmı kurcalamaya karşı korunaklı olmasına rağmen bu alan herkes tarafından okunabilmektedir (Peyrott, 2016).



Şekil 3.13. Veri Bilgisinin Decode Görünümü

Signature (İmza): Bir imzayı oluşturabilmek için Base64 ile kodlanmış başlık ve kodlanmış veri bilgisi ve gizli anahtar gereklidir. Bu bilgiler ile imzalama işlemi yapılır ve bu da JWT'nin son kısmına eklenir. Bu kısımda belirtilen imzalama algoritması başlıkta yer alır. HMACSHA256 yerine X.509 gibi genel ve gizli anahtar çifti ile de oluşturulan yapının başlık ve veri alanları birleştirilerek imzalanabilmektedir. Şekil 3.14'te HMACSHA256 ile imzalama fonksiyonu sonucunda üretilen kod JWT'nin son kısmına eklenmiştir.

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)
```

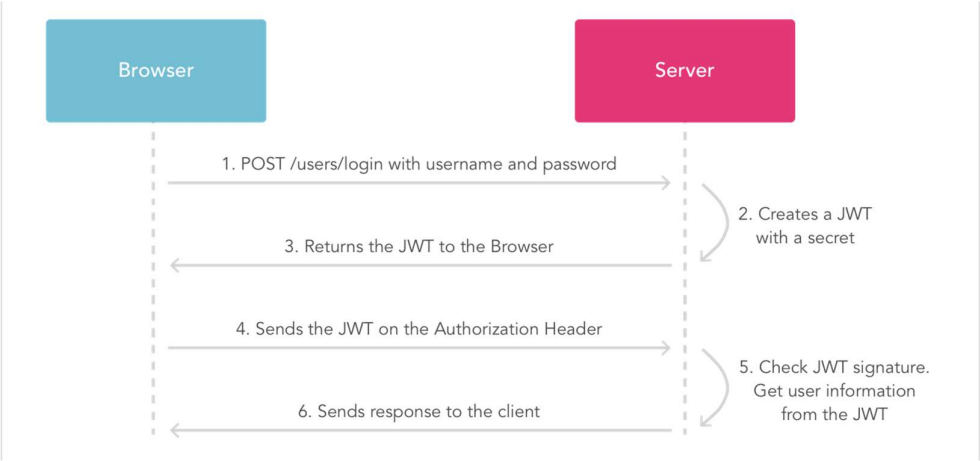
Şekil 3.14. İmza Verisi HMACSHA256 ile Kodlanması

JWT'nin geçerli olup olmadığı son kısımda yer alan imza kısmı doğrulanarak bulunur. Bu doğrulama sonucu alıcı ve gönderici arasında herhangi bir değişiklik olmadığı ve gönderen kişinin doğru olduğu bilgisi bulunur.

Bu çalışmada JSON Web Token içerisinde barındırdığı belirteçler ile sertifikalarda bulunan özellikleri simüle edebildiğinden, ek özellikler eklenebildiğinden ve daha hızlı doğrulanabilir olduğundan JWT yapısı tercih edilmiştir. İlerleyen zamanlarda şifreleme yönteminin değiştirilebilir olduğundan JWT'nin şifreleme algoritmasını değiştirme kolaylığı bulunduğundan çalışmada üretilen kanıt dosyasında JWT yapısı kullanılmaktadır.

3.8.6.2. JWT nasıl çalışır

Bir JWT yapısının çalışma mimarisinin iyi anlaşılabilmesi için bir uygulamaya login olunması ve iki taraf arasında (server – client ikilisi) iletişimin nasıl gerçekleştiği Şekil 3.15'te verilmiştir. (Kocabuga, 2021).



Şekil 3.15. JWT Çalışma Yapısı (Kocabuga, 2021).

Şekil 3.15'te gösterilen yapının aşamaları şu şekildedir;

1. Uygulamada işlem yapabilmek için kullanıcı adı ve şifre gerekmektedir. Bu işlem için kullanıcı bu bilgileri tarayıcı (browser) üzerinden HTTP post işlemi ile sunucuya gönderir.
2. Gönderilen kullanıcı adı ve şifre veri tabanı üzerinden doğrulanır ve bu bilgiler doğru ise server tarafından JWT üretimi gerçekleştirilir.
3. Server tarafından üretilen JWT bilgisi, bilgilerini gönderen kullanıcı tarafına gönderilir. Bundan sonraki işlemlerinde kullanıcı, sunucu ile arasındaki iletişimde üretilen JWT bilgisini kullanarak kullanıcı adı ve şifre doğrulamasını yapmasına gerek kalmayacaktır. JWT için tanımlanan bir son kullanım tarihi varsa bu tarihe kadar kullanıcı işlemlerini bu JWT yardımı ile yapacaktır.
4. Bundan sonraki işlemler HTTP üzerinden, JWT bilgisinin Authorization Header parametresine eklenerek yapılmaktadır.
5. Sunucu tarafından alınan JWT bilgisinin imzasının doğrulanma işlemi gerçekleştirilerek doğru olup olmadığı tespit edilir.
6. Geçerli JWT gönderilmiş ise Yetkilendirme işlemi onaylanır ve kullanıcıya server tarafından istediği bilgiler gönderilir.

JWT içeriğinde bilgileri taşıyabilme özelliği bulundurduğu için tekrar veri tabanına gitme ihtiyacı azalarak daha pratik bir yol sunmaktadır.

4. UYGULAMANIN DETAYLARI

Önerilen modelin daha iyi anlaşılabilmesi için uygulama detaylandırılarak anlatılmıştır. Uygulama beş aşamadan oluşmaktadır. Akıllı sözleşmenin yazılması, çalışma ortamının kurulması ve hesapların bağlanması, akıllı sözleşmenin blok zincirinde yayına alınması, merkezi olmayan uygulamanın (Decentralized Application- DApp) oluşturularak akıllı sözleşme ile bağlanması ve oluşturulan bu uygulamanın test aşaması ile son bulmaktadır.

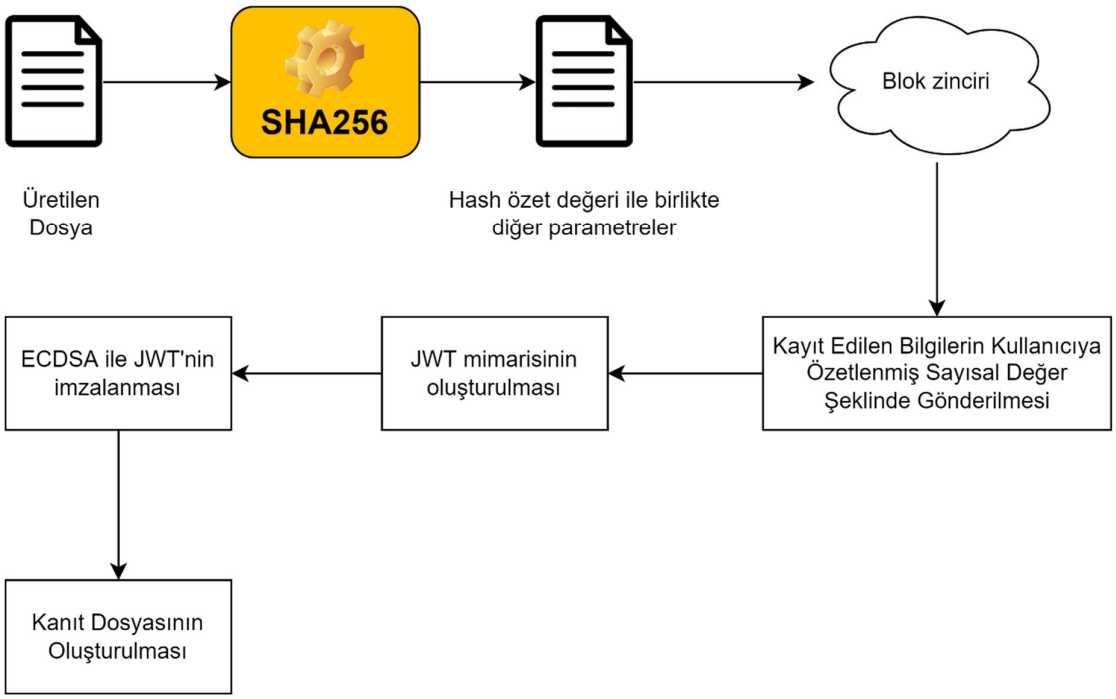
4.1 Önerilen Çalışma Modeli

Genellikle X.509 sertifikalar ile dosyalar imzalanabilmektedir. Bunlar ile dosyaların özet değerleri üretilmekte ve bazı bilgiler eklenerek bu bilgiler imzalanmaktadır. Yine aynı sertifika ile doğrulama işlemi gerçekleştirilebilmektedir. Bu çalışmada önerilen model ile standart olarak kullanılan sertifikalardan daha güçlü ve kullanımı basit ve hızlı bir yapı modeli sunulacaktır.

X.509 sertifikalarında kullanılan RSA yöntemi genellikle 2048 bit anahtar uzunluğuna sahip olduğundan güvenlik düzeyini artırmak istediğimizde anahtar boyutunu artırmamız gerekmektedir. RSA anahtar uzunluk (bit) değeri artırıldığında üretim ve doğrulanma süreci artacağından bu modelde ECDSA algoritması kullanılmıştır. Hem anahtar boyutu hem sağladığı güvenlik açısından bu şifreleme algoritması tercih edilmiştir.

Bu model ile blok zincirinde tutulacak dosya özet değeri ile karşılaştırılma yapılması için JWT yapısı ve ECDSA şifreleme yöntemi birleştirilecek ve yeni bir doğrulama yöntemi sunulacaktır.

Şekil 4.1'de bu çalışmada önerilen doğrulama modeli şema olarak gösterilmiştir. Orijinal dosya SHA256 algoritmasından geçirilerek bir özet değeri üretilir. Özet değeri ile imzalayacak kişinin blok zincirindeki açık adresi ve istenilen diğer kişisel özellikler ile blok zincirine gönderilir. Blok zincirinde yer alan akıllı sözleşmeye gelen bu bilgiler imzalama algoritmasının tipi, özetleme fonksiyonunun adı, bunu hangi akıllı sözleşme adresi üzerinden yaptığının bilgisi, gönderen kişinin blok zincirindeki açık adresi ve zaman damgası ile tekrar özetleme değeri üreterek karşı tarafa bu özet değeri ve diğer bilgilerin tamamını geri döndürülür.



Şekil 4.1. Önerilen Model Çalışma Prensibi.

Blok zinciri üzerinde dosya özet değeri, üretilme süresi ve üretilen bilgilerin özet değeri tutulur. Gönderilen değer kullanıcı tarafındaki sözleşmeyi çalıştıran merkeziyetsiz uygulama üzerinde JWT yapısını oluşturmak için gönderilen değerler ile bu değerlerin aldığı bilgilerin özetini JWT mimarisinde başlık ve veri alanına denk gelen kısımda toplanır.

Şekil 4.2'de ve Şekil 4.3'te verilen başlık bilgisi ve veri bilgisi birleştirilir ve gönderen kişinin gizli anahtarı ile üretilen ECDSA anahtar çifti kullanılarak şifrelenir. Bu şifrelemenin sonucunda kanıt dosyası üretilmiş olur.

```
{
  "alg": "ES256",
  "typ": "JWT"
}
```

Şekil 4.2. Önerilen Model Başlık Bilgisi.

```
{
  "hash": "8e9066215774fa39348ca71aef5856035432d6cf1bf233d959f7a597eb840aed",
  "senderAddress": "0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266",
  "name": "Muhammet Mustafa TOZLU",
  "contractAddress": "0xcf7ed3acca5a467e9e704c703e8d87f634fb0fc9",
  "iat": 1658735268,
  "verifyHash": "506e069fb67ff1251e29b5f7fe429a4d216ffebb6d5742b55e254e8d54bd0f77"
}
```


Şekil 4.3. Önerilen Model Veri Bilgisi.

Doğrulama işlemi, orijinal dosyanın aynı kontrat adresine özet değerini göndermesi ile teyit edebileceği gibi aynı işlemi oluşturulan kanıt dosyası ile de gerçekleştirilebilir. Bu ilk işlem arasındaki fark orijinal dosya tek başına gönderildiğinde ne zaman üretildiği ve tüm diğer bilgilerin alınıp işlendiği doğrulama özet değerine ulaşabilir. Kanıt dosyası daha kapsamlı geniş bilgi verebilmektedir. Bunun için gönderen taraf, JWT bilgisini içeren kanıt dosyası ile orijinal dosyayı paylaşacağı kişiye göndermesi ve doğrulama işlemini yapacağı ECDSA anahtar çiftinden açık anahtarı paylaşması gereklidir.

Bu çalışma kapsamında oluşturulan kanıt dosyasında doğrulama işleminde fazla verilerin ayrı ayrı saklanması yük oluşturabileceğinden kanıt dosyasına açık anahtar da eklenilmiştir. Geliştirilen merkeziyetsiz uygulama tarafından orijinal dosya ve kanıt dosyası kullanılarak sistem tarafından doğrulama sağlanabilmektedir. Burada gerçekleşen işlemler bu uygulama kullanılmadan yapılması gereken işlemler ile aynıdır.

Bu uygulama kapsamında geliştirilen merkeziyetsiz uygulama kullanılmadan da teyit edilebilme özelliği merkeziyetsiz bir yapının gerekliliği olduğu için bu çalışma kapsamında geliştirilen merkeziyetsiz uygulama üzerinden doğrulama yapmak istemeyen alıcılar olabildiği düşünülmüştür. Bunun için JWT yapısına kontrat adresi de dahil edilerek kanıt dosyası üretilmiştir. Kanıt dosyasını alan alıcı ilk olarak JWT kanıt dosyasının üretildiğini, gönderen kişi tarafından geldiğini teyit etmelidir. Sonrasında base64 formatı olarak çevrilebilen veri kısmını internetten bulabileceği ya da kendisinin yazabileceği bir script dosyası ile okunabilir bir hale çevirip özet değerini tutan “verifyHash” değeri çıkartılmalı ve sanki bir JWT yapısı imzalıyor gibi başlık ve veri kısmını nokta (.) ile birleştirerek (imzalama kısmı hariç) boşlukları tamamen kaldırıp tek bir metin haline getirerek SHA256 algoritması ile özet değeri üretmelidir. Sonrasında “verifyHash” değeri ile eşleşip eşleşmediğini kontrol etmelidir. Eğer eşleşme başarısız ise bu kanıt dosyası geçersizdir.

Eğer eşleşme başarılı ve “verifyHash” değeri ile uyuşuyorsa kontrat adresine orijinal dosyanın özet değeri üretilerek “verifyHash” değeri ile gönderilmelidir ve teyit edilmelidir. Teyit işlemi başarılı ise dosyanın orijinal olduğu ve üretildiği tarih bilgisi alıcıya gösterilmektedir. JWT kısmında bulunan diğer bilgilere bakılarak dosyayı üreten kişinin bilgilerine ulaşılabilmektedir.

Bu model sayesinde yeni güçlü bir elektronik sertifika üretimi gerçekleştirilmiştir. Sertifikaya ihtiyaç olmadan da herkes tarafından dosyanın ne zaman üretildiğinin kanıtı blok zincir sistemi ile bilinebilmektedir. Kanıt dosyası daha detaylı kapsamda içerik bilgisini görebilmek ve sahipliğinin üreten kişinin adına üretici kişinin blok zincirindeki açık anahtarını teyit edebilmek için gereklidir. Bu kanıt dosyası kullanıcıya verildikten sonra orijinal dosya ile saklanması gerekmektedir.

4.2. Uygulama Tanıtımı

Uygulamada önerilen yöntemin çalışma düzeninin anlatıldığı aşamadır. Yapılan uygulamada dikkat edilen yöntemler ve dijital eserin diğer dosyalardan farkının bulunması ve dijital eseri ilk kim üretti sorusuna cevaplar üretilmiştir.

4.2.1. Akıllı sözleşmenin yazılması

Blok zincirinin avantajlarından biri olan akıllı sözleşmeler ile oluşturulan kurallara göre çalışan ve her yerden erişimin mümkün olduğu yapılar kullanılmıştır. Bu çalışmada akıllı kontratta yer alması gereken özellikler belirlenmiştir. Öncelikle dijital eserin varlığının tespiti için gerekli olan eserin özet değeri (SHA-256 algoritması kullanarak oluşturulan) oluşturulur ve oluşan bu dijital değer belirlenir. Oluşan bu dijital değerin orijinal dosyayı temsil ettiği söylenebilir. Bu orijinal dosyanın dijital değeri (özeti) sadece sistemde var olup olmadığını tespit etmek için kullanılabilir.

Dijital eserin korunma aşaması bu dosyanın olup olmaması ile ilgilense de asıl sorun dosyayı ilk kimin ürettiğidir. Hatta dosya içeriği bir miktar değişse bile dijital özet değeri değiştiği için bir başkasının içeriği değiştirip tekrar oluşturulan uygulamaya yüklemesi engellenemez. Bu soruna cevap bulabilmek için ise ilk ne zaman üretildiğini bulabilmek gerekmektedir. Bu aşamada akıllı sözleşme eserin dijital değerinin yanına zaman damgasının tutabilecek bir özelliğin de eklenmesi gerektiği ihtiyacı çıkmaktadır. Literatüre bakıldığında bu geleneksel yöntemlerde dijital eserin özeti alındığı ve üretildiği

anda verilen bir zaman damgası ile tekrar özet değeri çıkarıldığı gözlemlenmiştir. Bu işlem için zaman damgası, dijital eserin özet değerini akıllı sözleşmeye gönderildiği anda blok zincirinin anlık olarak UTC (Eşgüdümlü Evrensel Zaman) zaman dilimine uygun değeri ekler.

Dijital eserin içeriğinin sistemde tutulmadığı için içeriği bilmezken onu tanımlayabilen ve parmak izi gibi görev gören bir dijital özet değerini tutmaktadır. Bu dijital özet değeri akıllı sözleşmeye ulaştığı anda zaman damgası verilmiştir. Bunun yanı sıra geleneksel yöntemlerde yer alan dijital eseri üreten kişinin de isminin alınıp verinin eşsiz bir şekilde tutulması sağlamak için yazar bilgisi eklenmiştir. Bunun yanı sıra bu belgeyi ilk tanımlayan kişinin blok zincir adresinin de işlenmesi bu sırada gerçekleştirilmiştir.

Gönderilen özet değerlerin işlenebilmesi için yazma işlemi metodu oluşturulmuştur. Bu metotta yukarıda bahsi geçen bilgiler doldurularak dijital özet değeri ile bir lineer listeye ataması gerçekleştirilmiştir. Bu işlem sırasında eğer daha önce özet değeri kayıtlı ise listeye doğrudan erişim ile kontrol edilip erişimin engellemesi için yapı kurulmuş ve yapılan işlemlerin geri alınması ile işlemin iptal edilmesi sağlanmıştır.

Doğrulama aşamasının gerçekleştirilebilmesi için okuma işleminin metodu oluşturulmuştur. Orijinal dosyanın tek yönlü şifrelenerek özet değeri çıkarılması ile sorgulama esnasında direkt erişim sağlanarak hızlı bir şekilde varlığı tespit edilebilmektedir. Tespiti sonrasında yazar ismi, eserin özet değeri ve oluşturulma zamanı olarak cevap dönmektedir. Oluşturulma süresi ile dosyanın hangi zamanda ilk kim tarafından üretildiğinin tespiti sağlanmaktadır. İlerleyen kısımda üretilen kanıt dosyasının kullanılması ile daha kapsamlı bilgilerin doğrulanabilmesi mümkündür.

4.2.2. Çalışma ortamının hazırlanması ve hesapların bağlanması

Hardhat'in sağladığı geliştirme ortamı kurulmuştur. Bu geliştirme aracının ile bir düğüm oluşturulmuş ve Hardhat lokal test ağında simüle edilmiştir. Test ağında kullanabilmek için test hesapları tanımlanmıştır.

MetaMask bir cüzdan entegresi olup, asıl Ethereum ağından, HardHat geliştirme ortamının sağladığı test ağına geçiş sağlanmıştır. Yine burada kolaylık sağlamak için verilen test hesaplarının özel anahtarları kullanılarak MetaMask'a tanımlama yapılmış ve kullanıma hazır hale getirilmiştir. Şekil 4.4'te MetaMask uygulamasına özel anahtar eklenerek hesaba erişim sağlanmaktadır.

Şekil 4.4. MetaMask Özel Anahtar ile Hesap Bağlama.

4.2.3. Akıllı sözleşmenin blok Zincirinde yayına alınması

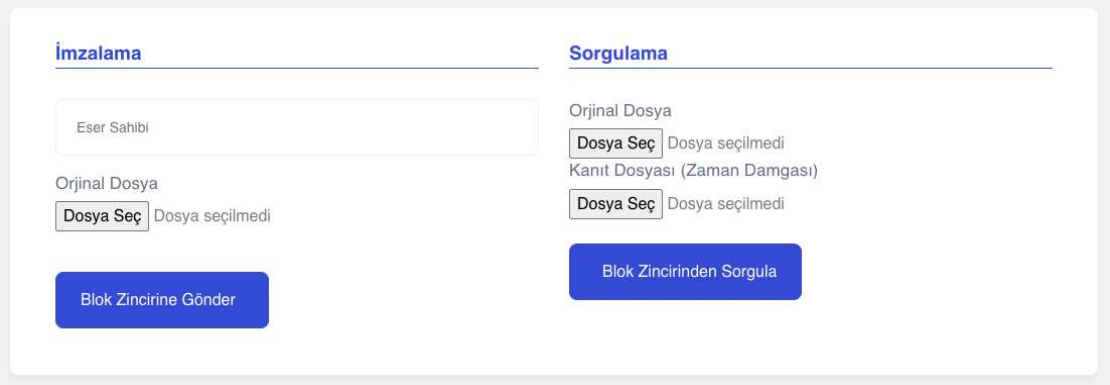
Kodlanan akıllı sözleşme Hardhat ile derlenmiştir. Derleme sonucunda oluşan ABI (Application Binary Interface) dosyasını geliştirilen merkeziyetsiz uygulama da kullanmak için kaydedilmiştir. Akıllı sözleşmenin yayına alınabilmesi için hardhat için gerekli script kodları yazılmış ve test ağında ilk oluşturulan test hesabı üzerinden yayına alınmıştır. Şekil 4.5'te görülebileceği üzere test ağı üzerinde akıllı sözleşme başarıyla yüklendikten sonra sözleşmenin adresi belirlenmiştir. Bu adres üzerinden sözleşmeye erişim yapan herkes tanımlanan fonksiyonları kullanabilmektedir.

```
Contract deployment: TimespanTez3
Contract address:    0xcf7ed3acca5a467e9e704c703e8d87f634fb0fc9
Transaction:         0x04f341445cccc354eb4de44f127d73bf6ec2df7ecbf9738149780c11ee3d9c82
From:                0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266
Value:               0 ETH
Gas used:            2473744 of 2473744
Block #4:            0x107242af8e5658158a7fdb4ac54b252e633b1636ad6e7f434c2dd8c6844b3b90
```

Şekil 4.5. Yazılan Akıllı Sözleşmenin Blok Zincire Gönderilmesi

4.2.4. DApp oluşturulması

Akıllı sözleşme ile haberleşecek bir DApp oluşturulmuştur. Bu uygulama ile ABI json dosyası eklenerek haberleşebilmesi sağlanmıştır. Şekil 4.6'de akıllı sözleşme ile bağlantı kuran DApp gösterilmiştir.

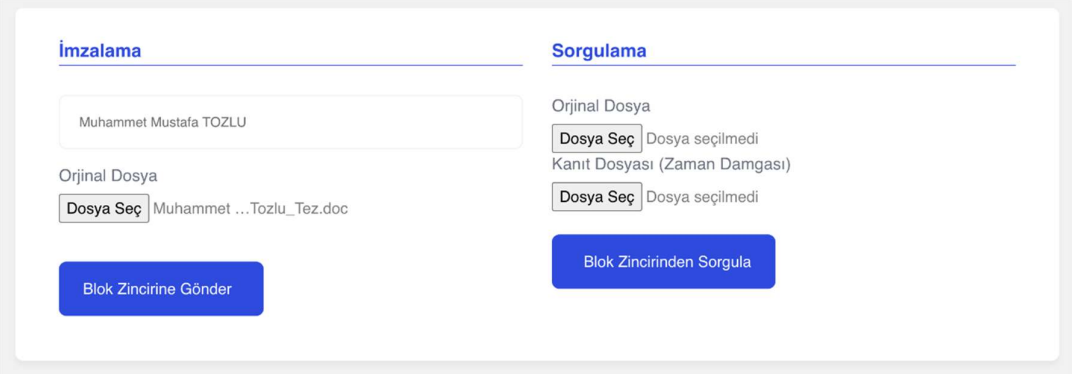


Şekil 4.6. Uygulama Görüntüsü

Eser sahibi adı ve orijinal dosya kullanıcıdan alınmıştır. Alınan dosyanın dijital özet değeri akıllı sözleşmeye gitmeden oluşturulmuş ve akıllı sözleşmeye gönderilmek için hazırlanmıştır. Bu sayede blok zincire gitmeyen dijital eser kopyalanma veya çalınma riskinden uzaklaştırılmıştır. Blok zinciri üzerinde bu işlemlerin blok zincirine yazılabilmesi için bir hesaba ihtiyaç bulunmaktadır. DApp ile bu hesabın bağlantısı MetaMask üzerinden sağlanmıştır.

4.2.5. Test ve sonuçları

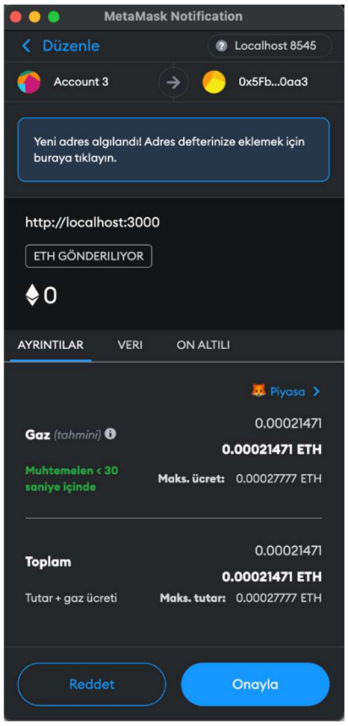
Şekil 4.7'de uygulamanın görüntüsü verilmiştir. Eser sahibi olarak Muhammet Mustafa TOZLU verilmiş ve örnek orijinal dosya olarak da bu tez çalışmasının belge hali eklenmiştir. Seçilen dosya akıllı sözleşmeye gönderilmeden önce SHA256 algoritmasından geçirilerek özet değeri oluşturulmaktadır. Yazar ismi ve dosya özet değeri DApp aracılığıyla akıllı sözleşmeye gönderilmektedir.



Şekil 4.7. Uygulamada Dosya İmzalama Aşaması

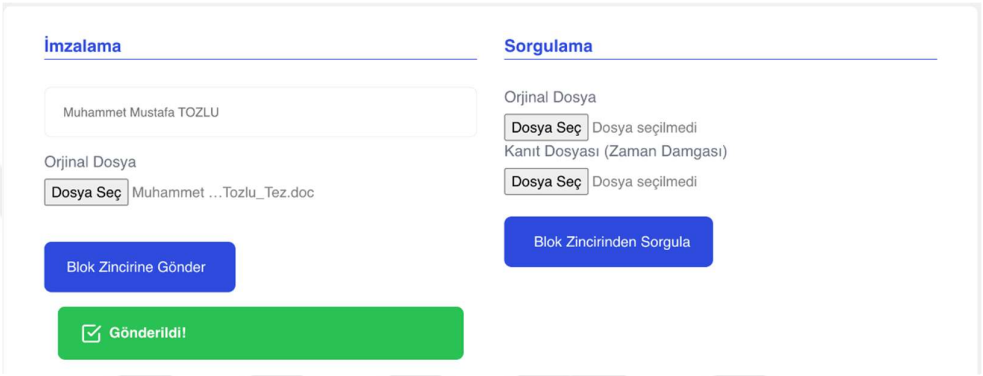
Gönderilen özet değeri daha önceden sistemde kayıtlı değil ise gönderen kişinin halka açık blok zincir adresi, akıllı sözleşme adresi, üretilme tarihi blok zincir UTC formatındaki saatine göre eklenmekte verifyHash değeri isminde tutularak doğrulama sağlanmaktadır. Yeni modele göre JWT yapısındaki başlık ve veri kısımları bytelara dönüştürülerek işlenmekte ve geri döndürülen cevap imzalanmamış JWT yapısındandır.

Şekil 4.8'de akıllı sözleşmede yazma işlemi başlatıldığını ve bu işlemin ücreti olduğunu MetaMask aracılığıyla göstermektedir. Bu işlem onaylandığında hesaptan o miktar kadar işlem ücreti düşmekte ve akıllı sözleşmede yazma işlemi gerçekleştirilmektedir.



Şekil 4.8. Akıllı Sözleşmede Yazma İşlem Ücreti MetaMask Görüntüsü

Oluşturulan test hesapları üzerinden MetaMask ile bağlanarak bu işlem ücreti onaylanmaktadır. Yapılan bu işlemin toplam ücreti Şekil 4.8'de gösterilmiştir ve 0.00021471 ETH işlem ücreti istenilmiştir. Bu işlemin ardından akıllı sözleşmeye giden verilerin başarıyla gönderildiği Şekil 4.9'da gösterilmektedir. Akıllı sözleşme ile onaylama sonrası kanıt dosyası üretilme işlemi başlanarak akıllı sözleşmeden döndürülen değerler ile kanıt dosyası oluşturulmuştur.



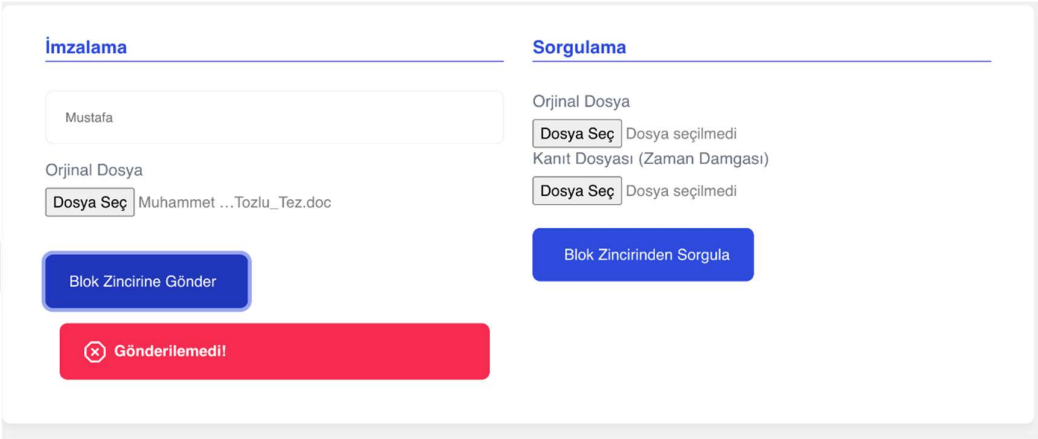
Şekil 4.9. DApp Üzerinden Akıllı Sözleşmeye Başarıyla Gönderildi Ekran Görüntüsü

Şekil 4.10'da kanıt dosyasının içeriği gösterilmiştir. Bu kanıt dosyası üretilmesi sırasında gönderen kişinin blok zinciri üzerindeki gizli anahtarı ile ECDSA algoritması kullanılarak şifrelenmiştir. Bunun doğrulamasını ise gönderen kişinin açık adresi ile yapılabilmektedir. Genellikle blok zincirde kullanılan eliptik eğri algoritması sabit ve standart olduğu için gizli anahtar verildiğinde açık anahtarı sabit olur. Açık anahtarı kanıt dosyası içerisinde JSON yapıda tutulmaktadır. Kanıt dosyası bu işlemi onaylamak için tek başına yeterli olsa da orijinal dosya ile karşılaştırılması gerekir bu yüzden paylaşılacak kişiye gönderilir.


```
{
    "proof": "eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.
    eyJoYXNoIjoiOGU5MDY2MjE1Nzc0ZmEzOTM0OGNhNzFhZWY1ODU2MDM1NDMyZDZjZjFiZjIzM2Q5NTlmN2
    E1OTdlYjg0MGFlZCIsInNlbmRlckFkZHJlc3MiOiIweGYzOWZkNmU1MWFhZDg4ZjZmNGNlNmFiODgyNzI3
    OWNmZmZiOTIyNjYiLCJuYW1lIjoiTXVoYW1tZXQgTXVzdGFmYSBUT1pMVSIsImNvbnRyYWN0QWRkcmVzcy
    I6IjB4Y2Y3ZWQzYWNjYTVhNDY3ZTllNzA0YzcwM2U4ZDg3ZjYzNGZiMGZjOSIsImlhdCI6MTY1ODczNTI2
    OCwidmVyaWZ5SGFzaCI6IjUwNmUwNjlmYjY3ZmYxMjUxZTI5YjVmN2ZlNDI5YTRkMjE2ZmZlYmI2ZDU3ND
    JiNTVlMjU0ZThkNTRiZDBmNzcifQ.
    Bds-B6phwavMoEQif1nxWgHWooVlT3OtIsDdMJcYQNgDlIcWIVKgZmBwymru2KOeaTLp-6Sbh2lNZf0Dvd
    hBLw",
    "publickey":
    "048318535B54105D4A7AAE60C08FC45F9687181B4FDFC625BD1A753FA7397FED753547F11CA869664
    6F2F3ACB08E31016AFAC23E630C5D11F59F61FEF57B0D2AA5"
}
```

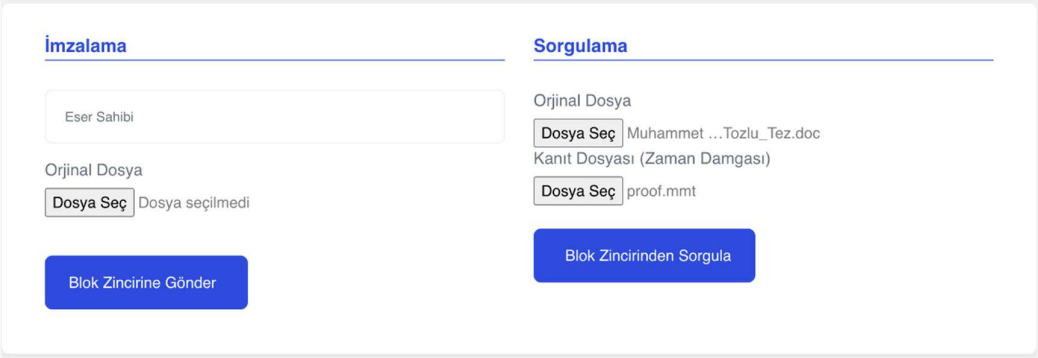

Şekil 4.10. Kanıt Dosyası

Şekil 4.11'de daha önce aynı dosya içeriği sisteme yüklenmişse tekrar yüklendiğinde yazma işlemi oluşturulmadan önce uyarı mesajı verilmektedir. Bu işlem daha önceden kaydedilen herhangi bir dosyanın özet değeri ile eşleşiyor ise meydana gelmektedir.



Şekil 4.11. Akıllı Sözleşmenin Ret Etme Aşaması Ekran Görüntüsü

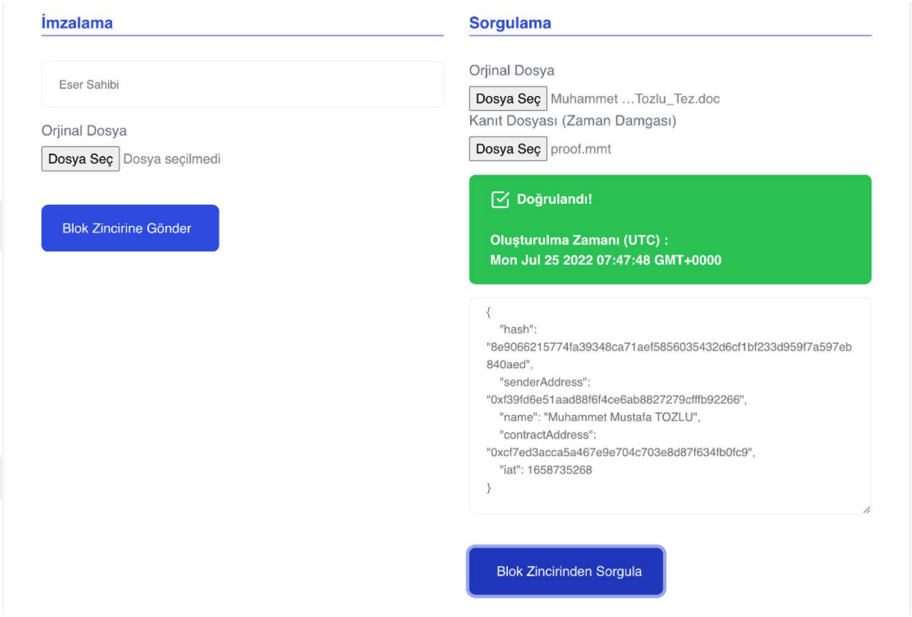
Şekil 4.12'de doğrulama aşaması ekran görüntüsüne yer verilmiştir. Orijinal dosya eklenir ve üretim sırasında oluşturulan kanıt dosyası seçilir. Eğer eser sahibinin dosyayı paylaştığı biri ise orijinal dosyayı alırken yanında verilen kanıt dosyasını eklenmelidir.



Şekil 4.12. Akıllı Sözleşmenin Doğrulama Aşaması Ekran Görüntüsü

4. bölümün 1.maddesin önerilen çalışma modeli anlatıldığı üzere önce proof dosyası kendi içerisinde doğrulaması sağlanır. Proof dosyasının içerisinde bulunan açık anahtar ile JWT yapısı doğrulanır. Eğer doğrulama başarılı ise base64 formatını

okunabilir hale çevirerek verifyHash değeri çıkartılır ve boşluksuz yapıda geriye kalan başlık ve veri kısmı birleştirilir. Özet değeri oluşturularak kanıt dosyasındaki verifyHash değeri ile eşleşip eşleşmediğine bakılır. Eşleşme sonucunda akıllı kontrata değerler gönderilir ve blok zinciri üzerinden de doğrulama sağlanır. Başarılı ise Şekil 4.13'teki gibi sistem bir doğrulama mesajı ile beraber oluşturma zamanı göstermektedir. JWT yapısındaki bilgileri de alt kısımda okunabilir halinde gösterilmektedir.



Şekil 4.13. Orijinal Dosyanın Kanıt Dosyası ile Doğrulanması

Kanıt dosyası hatalı ya da eşleşme bulunmadığın da Şekil 4.14'te gibi kanıt dosyası değiştirilmiştir mesajı verilmektedir. Doğrulama başarısız olmuştur.

Şekil 4.14. Orijinal Dosyanın Kanıt Dosyası ile Doğrulanması

Yukarıda anlatılan yöntemleri daha iyi incelemek için bir eser daha oluşturulmuş ve içerik eklenmiştir. Aynı eser kopyalanıp içeriklerinde ihmal edilebilecek derecede küçük değişiklikler yapılarak iki belge daha üretilmiştir. Dokümanlar blok zincirine kaydedilmiş ve karşılaştırmaları yapılmıştır. Belge1.docx uzantılı içerikten kopyalanan Belge2.docx ve Belge3.docx Çizelge 4.1.de verilmiştir. Sayısal Özet değerinin değiştiği tablo üzerinden görülmektedir.

Çizelge 4.1. Djital Eserlerin Sayısal Özet Değeri

Dijital Eser	Dijital Eserin Sayısal Özet Değeri
Belge1.docx	c3e95deb18e7fcb49912324463b4e2e0d4cef91a6ce256a13f92e90ff29254b4
Belge2.docx	b2e60da76d0c53147def42ec9f3a6585764f065869a18a137e57d1745f5e2649
Belge3.docx	63358c5b39c8fa12dac2ab232f0e0bb7b47d72f65aa09508db5dba1aaf377bef

Önerilen model üzerine blok zincirine Çizelge 4.1'de belirtilen dosyalar eklenmiş ve her bir dosya eklenirken eser sahibi adı verilmiştir. Eklenen dosyaların isimleri değişse bile içerikleri değişmediği sürece aynı dosya olarak tespit edilmiştir. Dosyaların içeriklerinde küçük değişiklikler yapılmış, sonucunda eserin sayısal özet değeri değişeceği için zaman damgasının önemi burada vurgulanmıştır. Akıllı sözleşmeye ulaşan veriler blok zincirinin zamanı ile sisteme kaydedilmiştir.

Modelde sayısal özet ile direkt erişim bulunduğundan üzerinden vakit geçse bile bu belgelere çok hızlı bir şekilde ulaşılabildiği gözlemlenmiştir. Ayrıca eser sahibi kim ve bu eseri ilk kim üretti sorusuna cevap üretilmiştir. Zaman damgası ile eserlerin sahibi ve üretildiği tarih bilinebilmektedir. Ekstra bilgileri de üretilen JWT mimarisinden imzalanmış ve açık bir halde kanıt dosyası olarak alınabilmektedir.

5. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Önerilen model, dijital eserlerin eser sahibinin belirlenebilmek ve bu belirleme sonrasında oluşabilecek eseri ilk üreten kişi kim sorusuna cevap verebilmeyi hedef almıştır. Önerilen model, örnek veriler ile test edilmiş, dosyaların şifrelenerek blok zincirinde saklanması ve bunların doğrulanabilir olması sağlanarak önerilen model tamamlanmıştır.

5.1. Tartışma

Önerilen modellerde yöntem seçimi ve verdiği güvenliğin güncel kullanılan algoritmalara göre karşılaştırılması yapılmıştır. Literatürde kullanılan yöntemlerden farklarına değinilmiştir.

5.1.1. Sertifika ve özel anahtarlar kullanan algoritmaların incelenmesi

Sertifikalarda güvenlik, şifreleme kimliği ile gerçekleşir. Güvenliğin sağlanabilmesi için güçlü özel bir anahtar ve güçlü bir sertifika kullanmak gereklidir.

Sertifika oluşturmak ve sertifikanın güvenliğini sağlayabilmek için sertifikayı imzalayacak özel anahtarın gücüne ve sayısal imza sırasında kullanılan kriptolojik yönteme bağlıdır. Sayısal imzalar ve web siteleri için de geçerli olan 2048 bitlik RSA özel anahtarı yeterli güvenlik sağlaması sonucu, RSA yaygın olarak kullanımı artmış ve varsayılan olarak tercih edilmesi sağlamıştır.

2048 bitlik bir RSA algoritmasının özel anahtarı yaklaşık olarak 112 bit güvenlik düzeyi sağlayabilmektedir. 128 bitlik bir güvenlik sağlayabilmek için ise 3072 bitlik bir RSA özel anahtarı kullanılması gerekmektedir. Bit sayısı ne kadar artarsa o oranda performans düşüklüğüne yol açmaktadır. 256 bit anahtar uzunluğuna sahip bir ECDSA'nın sağladığı güvenlik, 3072 bit anahtar uzunluğuna sahip bir RSA güvenliği ile eşdeğerdir. Anahtar uzunlukları karşılaştırıldığında ECDSA algoritması, RSA algoritmasına göre daha az uzunluğa sahip olmasına rağmen güvenliği aynı düzeydedir (Böge, 2018). ECDSA algoritması sistem kaynaklarını daha az tüketirken aynı güvenliği vermesi sebebiyle bu çalışmada dosyaların imzalaması aşamasında bu algoritmanın kullanılmasının yararlı olabileceği düşünülmüştür.

Çizelge 5.1'de görüldüğü gibi anahtar uzunluğuna göre sağlanan güvenlik değerleri gösterilmiştir. Bu algoritmalarda anahtar uzunluğu ne kadar büyük olursa o kadar fazla güvenlik sağlanmaktadır. Yalnız anahtar uzunluğu ne kadar artarsa o kadar işlem gücü artığından çok yüksek bir anahtar uzunluğu tercihi yapılmamalıdır.

Çizelge 5.1. RSA ve ECDSA Algoritmalarının Sağladığı Güvenlik Değerleri

Algoritma	Anahtar Uzunluğu (Bit)	Güvenlik (Bit)
RSA	1024	80
RSA	2048	112
RSA	3072	128
RSA	15360	256
ECDSA	163	80
ECDSA	224	112
ECDSA	256	128
ECDSA	521	256

5.1.2. Merkle kök değeri yerine akıllı sözleşme adresi

Bu çalışmaya benzeyen ve aynı amaca hizmet eden birçok çalışma mevcuttur. Bu çalışmalar yapılırken blok zinciri kullanılarak özet değerleri saklanmaktadır. Bu tez çalışması geleneksel yöntemleri kullanmadan dosyaların saklanabileceğini ve doğrulama yöntemlerinin farklı bir şekilde yapılabileceğinden bahsedilmektedir.

Ayrıca bazı çalışmalarda yeni bir blok oluşturulmadan önce tüm farklı dosyalar toplanarak özet değerleri oluşturulmakta ve oluşan son özet değerinden bir cüzdan adresi üretilerek küçük miktarda para transferi ile başka bir cüzdana gönderilmektedir. Bu işlemler bloklar doğrulandığında geçerlilik kazanmaktadır. Yapılan işlemleri doğrulayabilmek Merkle kök değerinin eşleşmesi ile mümkün olmaktadır. Aynı zamanda bu değerler bloklar blok zincirinde mutabakatların doğrulanması durumunda geçerlilik kazanmaktadır.

Bu çalışmada kapsamında Merkle kök değeri yerine doğrulama işlemini akıllı sözleşme ile yapılabilmektedir. Oluşturulan kanıt dosyasında yer alan akıllı sözleşme adresi ile herhangi bir yerden blok zincirine dahil olarak işlemlerin doğrulanabilmesi mümkündür. Kanıt dosyasında bulunan zaman değeri akıllı sözleşmeye ulaştığında blok zincirinin o anki zaman değeri olduğundan blok zincirinin gecikmeli blok doğrulama süresinden etkilenmeden yaklaşık olarak gerçek oluşturulma süresini de verebilmektedir.

5.1.3. Geleneksel yöntemlerde sertifika otoritesi (CA) gerekliliği

Bu çalışma ile gereken CA gerekliliği ortadan kaldırılmıştır. Dışarıdan herhangi bir sertifika oluşturulmadan bu işlem akıllı sözleşme ve DApp aracılığıyla gerçekleşmektedir. JWT yapısının kendi belirteçleri ile sertifika yapısının içerdiği özelliklere benzerlik göstermektedir. Aynı zamanda sertifikaların yaygın olarak kullandığı RSA algoritması performans ve güvenlik söz konusu olduğundan anahtar uzunluğu 2048 bit olarak belirlenmiştir. Yapılan yeni yöntem sayesinde ECDSA kullanımı performans ve güvenlik düzeyini artırdığından CA gerekliliği kalmamıştır.

Ayrıca geleneksel yöntemlerde yer alan Sertifika İptal Listesi (SİL) sertifikaların geçerliliğini doğrulama girişiminde bulunan kişilere, bilgisayarlara ve uygulamalara iptal edilen sertifikalar hakkında bilgi dağıtmak için kullanılır. Bu tez çalışmasında bu sistem kullanılmayarak literatürden farklı yaklaşım da bulunarak ek iş yüklerinden kurtarmakta ve sadece doğrulamaya odaklanmaktadır. Kanıt dosyasında doğrulayacak açık anahtar içerisinde yer aldığından bu ek işlemlere gerek kalmadan doğrulama gerçekleşmektedir.

5.1.4. Özel doğrulama sertifikası: JWT ve ECDSA birleşimi

Bu çalışma kapsamında özel doğrulanabilir bir sertifika modeli önerilmiş ve bu model kanıt dosyası olarak kullanılmıştır. Blok zincirinde orijinal dosyanın içerdiği ekstra bilgilerin özet değerine ve ne zaman üretildiğin bilgisine erişilmesi yeterlidir.

Blok zincirindeki işlemler sonrası kullanıcıya döndürülen bilgilerin kanıt dosyası olarak oluşturulması blok zinciri dışında gerçekleştirilir. Bu kanıt dosyası ile orijinal dosyanın kim tarafından üretildiği, hangi kontrat adresinden üretildiği, hangi alıcı tarafından üretildiği gibi bilgilere erişilmesi sağlanmaktadır. ECDSA şifreleme için anahtar çifti gerektirdiği için gizli anahtarın kontrat üzerine gönderilmeden blok zinciri dışında şifrelenmesi ve gönderen kişiye kanıt dosyası olarak oluşturulması sağlanmıştır.

Buradaki bu kanıt dosyasının bir başkası tarafından tekrardan üretilebileceği göz önüne alınarak, gönderen kişinin açık adresi ve kontrat adresi alınıp diğer bilgiler ile işleme tabi tutularak parmak izi gibi bir özet değeri oluşturulmuştur. Bu işlem sayısal imzalamadan sonra değişikliği tespit edebilmektedir. JWT yapısının hızlı ve küçük boyutlu olmasının getirdiği avantaj ve ECDSA şifreleme yönteminin getirdiği güvenlik ve bu birleşimin hızlı doğrulanabilir olması ilerleyen zamanlarda diğer sayısal imzalama yöntemlerinde de kullanılabileceğinin önünü açmaktadır.

Ayrıca bu mimari ile kuantum sistemlerin ortaya çıkması ile geliştirilebilecek şifreleme yöntemleri ile çalışabilecek bir yapıda kurulmaktadır. ECDSA yerine farklı bir şifreleme yöntemi ile burada kullanılan yeni sertifika doğrulama yönteminin şifreleme gücü artırılabilecektir. Aynı şekilde bu kanıt dosyası X.509 sertifikalarının yaygın olarak kullandığı şifreleme yönteminden daha güçlü bir şifreleme yöntemine sahip olduğundan adli süreçte delil olarak kullanılabileceği düşünülmektedir.

5.2. Araştırma Sonuçları

Dijital eserin varlığı kadar ilk olarak kim tarafından ve ne zaman üretildiği de önemli bir bilgidir. Bu bilgilerin kalıcı olarak saklanabilmesi için Haber ve Stornetta (1990), tarafından dijital eserlere zaman damgası ekleme yöntemini öne sürmüşlerdir. Bu sistem geliştirilerek blok zinciri üzerinde uygulanmaya başlanmıştır. Blok zincirinin getirdiği avantajlardan biri olan zaman damgası kullanılmış ve bloklara gönderilen veriler zaman damgası ile imzalanmıştır.

Bu çalışmada önerilen blok zinciri modeli dijital eserleri zaman damgası ile ilk eseri üreten sahibine ulaştırabilmektedir. Une (2001), çalışmasında bahsettiği gibi aslında TSS modelindeki zincir sistemini burada blok zincirinin kendisi yapmaktadır. Bu model manipülasyonu minimize hale getirildiği öne sürülmüştür. Bu çalışma ile de başka bir DApp'den erişilmeye çalışılsa da akıllı sözleşme üzerindeki engelleyici yapı sayesinde aynı özet değerine sahip belgelerin tekrar yüklenmesi önlenmiş ve güvenlik sağlandığı görülmüştür. Merkle kök değeri yerine doğrulamayı akıllı sözleşme adresi üzerinden gerçekleştirilmesi sağlanmıştır. Oluşturulan kanıt dosyası içeriğinde akıllı sözleşme adresi hem zaman damgası hem de dijital dosyanın özet değeri ile tutulmaktadır. Bu da bütünlüğünü ve değiştirilmediğini garanti altına almaktadır.

Hyla ve Pejaś (2020), tarafından yapılan çalışma da bahsettiği gibi bu çalışmada doğrulanan verilerin kısa süreli sertifika değişimi yapması sorunu ortadan kaldırılmış ve biten sertifikalar için tekrar işlem yapılma yükü ortadan kaldırılmıştır. Hyla ve Pejaś gibi bu çalışma da sertifikayı tekrar güncelleme gibi iş yüklerini ortadan kaldırmayı hedef almış ve gözlemlenen sonuçlara göre başarılı olduğu görülmüştür. Program çıktılarına bakılarak önerilen sistem adımlarının hiçbirinde bir hatayla karşılaşılmadığı ve sistemin hızlı çalıştığı gözlemlenmiştir.

6. SONUÇLAR VE ÖNERİLER

Dijital eserleri kriptografik yöntemler kullanılarak geri döndürülemez bir özet değeri çıkarılmıştır. Bu çıkarılan özet değeri ile blok zinciri sistemi kullanılarak çalışmanın asıl amacı olan telif hakkının kime ait olduğunun tespiti kolaylaşmıştır. Fikri ürünlerin üretilmesinin büyük çabalar ile yapılması, üretilen ürünlerin ekonomik değerlerinin olması da korunmayı gerektirmiştir. Öncelikle korunması amaçlanan fikri ürünlerin değiştirilemez şekilde özet değerleri belirlenmiş. Bu özet değerlerin içerisinde eser sahibinin bilgileri de aynı zamanda verilmiştir. Böylelikle fikri ürünün yani eserin kime ait olduğu konusundaki tartışma sona ermiştir.

Diğer tartışma konusu olarak aynı fikri ürünün başkası tarafından üretilip üretilemeyeceğidir. Kriptografik yöntemler kullanıldığından dolayı bir özet değer çıkarılmaktadır. Tamamen benzer olarak üretilmiş bir fikri ürünün kopyalanması sistem tarafından izin verilmemektedir. Sisteme yüklenen dosyanın özet değeri daha önceden kaydedilmiş ise sistem hata mesajı yayınlayarak ürünün kime ait olduğunu bildirmektedir. Sistemin benzer nitelikle ancak farklı şekilde değiştirilmiş olduğu bir üründe ise koruması özet değer üzerinden olamayacaktır. Bu noktada da blok zinciri sisteminde üretilen özet değerin hangi zaman diliminde üretildiğinin belirlenebilir olması ile sağlanmıştır. Blok zinciri sisteminde bir ürün üretildiği zaman hangi zaman diliminde üretildiği değiştirilemez şekilde onaylanmaktadır. Bunu sistem kendi içerisinde saklamakta ve sonrasında aynı özet değerlerin sisteme girildiğinde bu bilgi doğrulanarak gösterilmektedir.

Türkiye'de geleneksel yöntemlerde kullanılan eser korunması merkezi otoriteye sahip sistemler üzerinden yapılmaktadır. Blok zinciri ile gelen şeffaflık, herkese açık olması, zincir yöntemi ile blokların birbirine bağlı olmasının getirdiği özellik ile merkeziyetsiz, herkesin güvenebileceği, manipülasyonların yapılması riskinin az olduğu bir öneri sunulmuştur.

Fikri ürünün korunmasında sistem ürün sahibinin sahiplik bilgilerini saklamakta ve zaman olarak önceliğini belirlemektedir. Blok zinciri kullanıldığı için veriler üzerindeki manipülasyonun neredeyse imkânsız olması nedeniyle telif haklarının korunması kapsamında bu çalışma Türkiye'de adli süreçlerde yardımcı olabileceği düşünülmektedir. Korumanın sağladığı yararlardan bir diğeri eserlerin çalınmasını ve dağıtılmasını önlemektedir.

Bu çalışmada lokal test ağı kullanılsa da sonraki çalışmalar da katılımcı sayısı geniş test ağında yayına alınacak ve testler yapılacaktır. Ayrıca bu model için depolama çözümü kullanılmamış ve sadece dosyaların sayısal özet değerleri ile işlem yapılmıştır. Kullanıcıların kanıt dosyası üretip bunu kendi gizli anahtarları ile imzalamaları sağlanmıştır. Sonraki çalışmalarda bununla ilgili güvenli zaman damgaları üretirken bu dosyalara erişim yapılabilmesi düşünülmektedir. İlerleyen zamanlarda yapılabilecek depolama işleminin getireceği özellikle belgeler güvenle saklanabilecek ve tapu işlemleri, araç alım satımı gibi noterde yapılabilecek birçok işlemi kolaylıkla ve hızlı bir şekilde gerçekleştirilebilecektir.

Bir başka çalışma olarak yapılabilecek ve birden fazla cüzdan ile imzalama teknolojisi entegre edilerek elektronik belge yönetimi gibi uygulamalarının, blok zinciri üzerine aktarılarak güvenli, doğrulanmış ve zaman damgalı olarak kullanılabileceği düşünülmektedir. Bunların yanı sıra akıllı sözleşme optimize edilip performansı artırılacak ve işlem ücretlerinin düşürülmesi sağlanacaktır.

KAYNAKLAR

Aghayev, H., 2021, Dijital platformlarda telif hakları ve yazılı eserler için blockchain tabanlı bir telif hakkı modeli, Yüksek Lisans, *Marmara Universitesi (Turkey)*, 105.

Akben, S. B. ve Subaşı, A., 2005, RSA ve eliptik eğri algoritmasının performans karşılaştırması, *KSÜ Fen ve Mühendislik Dergisi*, 8 (1), 35-40.

Akyüz, Y., 2021, Kripto para ve blokzincir teknolojilerinde kullanılan imzalama algoritmalarının analizi, *Marmara Universitesi (Turkey)*.

Alpago, H., 2018, Bitcoin'den Selfcoin'e kripto para, *Uluslararası Bilimsel Araştırmalar Dergisi (IBAD)*, 3 (2), 411-428.

Altuncu, E., 2019, Blokzincir kullanılarak kimlik doğrulama seremonisini ortadan kaldıran bir güvenli mesajlaşma uygulamasının geliştirilmesi, Yüksek Lisans, *TOBB ETÜ Fen Bilimleri Enstitüsü*, 80.

Alyaz, U., 2021, Blok zinciri tabanlı gerçek zamanlı çevrimiçi oylama sistemi önerisi, Yüksek Lisans, *İstanbul Aydın Üniversitesi*, 67.

Ata, B., 2019, Google trends verileri ile kripto para ilişkisi: Bitcoin örneği, Yüksek Lisans, *Burdur Mehmet Akif Ersoy Üniversitesi*.

Ayberkin, D., Beştaş, M. ve Üstün, Ö., 2018, Blok zinciri ile gerçek zamanlı doğrulanabilir eğitim belgeleri, *İktisadi Yenilik Dergisi*, 5 (2), 75-82.

Aydın, M. E., 2018, Blokzincir tabanli oy verme sistemi önerisi, Yüksek Lisans, *Necmettin Erbakan University (Turkey)*.

Babaoğlu, C. ve Karasoy, H., 2022, Kamu yönetiminde blokzincir: Kullanım alanları ve örnek uygulamalar, *Sosyoekonomi*, 30 (52), 283-297.

Beşkirli, A., Özdemir, D. ve Beşkirli, M., 2019, Şifreleme yöntemleri ve RSA algoritması üzerine bir inceleme, *Avrupa Bilim ve Teknoloji Dergisi*, 284-291.

Binance Academy, 2018, Blockchain avantaj ve dezavantajları, https://academy.binance.com/tr/articles/positives-and-negatives-of-blockchain: [30/05/2022].

Böge, S., 2018, Sanal özel ağlarda veri güvenliği, Yüksek Lisans, *KTO Karatay Üniversitesi*.

Bote, A., 2021, RSA algorithm in cryptography, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/: [12.06.2022].

Buterin, V., 2014, A next-generation smart contract and decentralized application platform, *white paper*, 3 (37), 2.1.

Çarkacıoğlu, A., 2016, Kripto-para bitcoin, *Sermaye piyasası kurulu araştırma dairesi araştırma raporu*.

Clark, J. ve Essex, A., 2012, Commitcoin: Carbon dating commitments with bitcoin, *International conference on financial cryptography and data security*, 390-398.

Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S. ve Nicholas, R., 2005, Internet x. 509 public key infrastructure: Certification path building, *Network working group, RFC*, 4158.

Demir, E. M., 2019, Yeni iletişim teknolojileri bağlamında fikri mülkiyet, *Kastamonu İletişim Araştırmaları Dergisi* (2), 35-48.

Efendioğlu, M. A., 2020, Cari mutabakat ve ödeme işlemleri için ethereum tabanlı blokzincir teknolojisinin kullanımının önerilmesi, *Lisansüstü Eğitim Enstitüsü*.

Ferwana, E. A., 2021, A blockchain-based tracking system for university donation, Yüksek Lisans, *Karabük Üniversitesi*.

FSEK, 1951, Fikir ve Sanat Eserleri Kanunu (Kanun No. 5846). Resmî Gazete 7981 (13 Aralık 1951). https://kms.kaysis.gov.tr/Home/Goster/33768: [18/07/2022].

Gerdan, G., 2019, Blokzincir teknolojisiyle gıda güvenliği ve yumurta sektörü için örnek bir uygulama, Yüksek Lisans, *Marmara Universitesi (Turkey)*.

Gipp, B., Meuschke, N. ve Gernandt, A., 2015, Decentralized trusted timestamping using the crypto currency bitcoin, *arXiv preprint arXiv:1502.04015*.

Gökhan, Ü. ve Uluyol, Ç., 2020, Blok zinciri teknolojisi, *Bilişim Teknolojileri Dergisi*, 13 (2), 167-175.

Gültekin, Y. ve Bulut, Y., 2016, Bitcoin ekonomisi: Bitcoin eko-sisteminden doğan yeni sektörler ve analizi, *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 3 (3), 82-92.

Gündüzgil, İ., 2021, Elektronik delillerin adli süreçteki aşamlarına uygun blok zinciri uygulaması geliştirilmesi, Yüksek Lisans, *Fırat Üniversitesi*.

Güven, V. ve Şahinöz, E., 2018, Blokzincir kripto paralar Bitcoin: Satoshi dünyayı değiştiriyor, *İstanbul: Kronik Kitap*.

Haber, S. ve Stornetta, W. S., 1990, How to time-stamp a digital document, *Conference on the Theory and Application of Cryptography*, 437-455.

Hasan, H. R. ve Salah, K., 2018, Proof of delivery of digital assets using blockchain and smart contracts, *IEEE Access*, 6, 65439-65448.

Hasırcıoğlu, I. ve Öz, D., 2008, Yapılandırılabilir ve dinamik bir sertifika doğrulama kütüphanesi modeli, https://www.emo.org.tr/ekler/a44180ab9ab950e_ek.pdf: [11/06/2022].

Hepp, T., Schoenhals, A., Gondek, C. ve Gipp, B., 2018, OriginStamp: A blockchain-backed system for decentralized trusted timestamping, *it-Information Technology*, 60 (5-6), 273-281.

Hyla, T. ve Pejaś, J., 2020, Long-term verification of signatures based on a blockchain, *Computers & Electrical Engineering*, 81, 106523.

İkizoğlu, E. Y., 2019, Türkiye standartlarına uygun blokzincir tabanlı diploma yönetimi, Yüksek Lisans, *İstanbul Şehir Üniversitesi*.

İslam, A., 2019, Blok zinciri teknolojisi ve kripto paralar: Mevcut durum, potansiyel ve risk analizi, *Marmara Universitesi (Turkey)*.

Johnson, D., Menezes, A. ve Vanstone, S., 2001, The elliptic curve digital signature algorithm (ECDSA), *International journal of information security*, 1 (1), 36-63.

Jones, M., Bradley, J. ve Sakimura, N., 2015, Json web token (jwt).

KAMU SM, 2021, Kamu SM zaman damgası nasıl çalışır?, https://kamusm.bilgem.tubitak.gov.tr/urunler/zaman_damgasi/kamu_sm_zaman_damgasi_nasil_calisir.jsp: [28/05/2022].

Kaya, Ö. F., 2020, Gayrimenkul sertifikalarının blokzincir ile entegrasyonu, Yüksek Lisans, *İstanbul Ticaret ÜniversitesiFen Bilimleri Enstitüsü*.

Kocabuga, E., 2021, JSON Web Token (JWT) nedir? Nasıl kullanılır?, https://erhankocabuga.com/json-web-token-jwt-nedir: [06/06/2022].

Kodaz, H. ve Botsalı, F. M., 2010, Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması, *Selcuk University Journal of Engineering Sciences*, 9 (1), 10-23.

Mendi, A. F. ve Çabuk, A., 2018, Bitcoin'in arkasındaki güç: Blokchain, *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, 1 (1), 12-23.

Nakamoto, S., 2008, Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review*, 21260.

Oğuzhan, T. ve Kiani, F., 2018, Blok zinciri teknolojisine yapılan saldırılar üzerine bir inceleme, *Bilişim Teknolojileri Dergisi*, 11 (4), 369-382.

Peyrott, S., 2016, The JWT handbook, *Auth0 Inc.: Bellevue, WA, USA*, 2017.

Rahmatulloh, A., Sulastri, H. ve Nugroho, R., 2018, Keamanan RESTful web service menggunakan JSON Web Token (JWT) HMAC SHA-512, *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, 7 (2), 131-137.

Sarıtaş, H., 2010, Dijital imza uygulamasının eliptik eğri şifreleme yöntemi kullanılarak gerçekleştirilmesi, Yüksek Lisans, *Marmara Universitesi (Turkey)*.

Sectigo, 2021, What is an X.509 certificate & How does it work?, https://sectigo.com/resource-library/what-is-x509-certificate: [10/06/2022].

Şenkardeş, C., 2021, Block-chain technology and NFT's: a review in music industry, *Journal of Management, Marketing and Logistics (JMML)*, 8 (3), 154-163.

Sert, M., 2008, Elektronik belgeler ve telif hakları, Yüksek Lisans, *Marmara Universitesi (Turkey)*.

Torun, A., 2017, Hierarchical blockchain architecture for a relaxed hegemony on cadastre data management and update: A case study for Turkey, *Proceedings of the UCTEA International Geographical Information Systems Congress, Adana, Turkey*, 15-18.

Une, M., 2001, The security evaluation of time stamping schemes: The present situation and studies, *IMES Discussion Papers Series 2001-E-18*.

Usta, A. ve Doğantekin, S., 2017, Blockchain 101 (2. bs), *Bankalararası Kart Merkezi*

Usta, E., 2022, Hardhat nedir? Nasıl kullanılır?, https://www.erayusta.com/hardhat-nedir-nasil-kullanilir/: [20/04/2022].

Varma, A., 2020, x.509 vs ECDSA vs RSA, https://www.anujvarma.com/x-509-vs-ecdsa-vs-rsa/: [07/06/2022].

Vikipedi, 2022, X.509, https://tr.wikipedia.org/wiki/X.509: [12/06/2022].

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A. ve Kishigami, J. J., 2015, Blockchain contract: A complete consensus using blockchain, *2015 IEEE 4th global conference on consumer electronics (GCCE)*, 577-578.

Yavuz, M., 2019, Ekonomide Dijital Dönüşüm: Blokchain teknolojisi ve uygulama üzerine bir inceleme, *Finans Ekonomi ve Sosyal Araştırmalar Dergisi*, 4 (1), 15-29.

Yıldız, R. ve Baştuğ, S., 2018, Blok zincir teknolojisi kapsamında elektronik konşimento.(ss. 7-12). IV, *ULUSLARARASI KAFKASYA–ORTA ASYA DIŞ TİCARET VE LOJİSTİK KONGRESİ. Düzenleyen Adnan Menderes Üniversitesi. Aydın*, 7-8.

Yılmaz, R., 2019, Ürünlerin tedarikçiden tüketiciye ulaşmasını takip edecek bir blok zinciri sisteminin tasarlanması, *İstanbul Üniversitesi*.

Zhang, Y., Xu, C., Li, H., Yang, H. ve Shen, X., 2019, Chronos: secure and accurate time-stamping scheme for digital files via blockchain, *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, 1-6.

Zheng, Z., Xie, S., Dai, H., Chen, X. ve Wang, H., 2017, An overview of blockchain technology: Architecture, consensus, and future trends, *2017 IEEE international congress on big data (BigData congress)*, 557-564.