T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOCKCHAIN TEKNOLOJİSİYLE AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK SERTİFİKA DURUM BİLGİLERİNİN YÖNETİLMESİ

YÜKSEK LİSANS TEZİ

GALİP ÇAĞAN NASUHOĞLU

Enstitü Anabilim Dalı	**:**	**ELEKTRİK – ELEKTRONİK MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Dr. Öğr. Üyesi Mustafa Zahid YILDIZ**

Mayıs 2019

T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOCKCHAIN TEKNOLOJİSİYLE AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK SERTİFİKA DURUM BİLGİLERİNİN YÖNETİLMESİ

YÜKSEK LİSANS TEZİ

Galip Çağan NASUHOĞLU

Enstitü Anabilim Dalı : ELEKTRİK – ELEKTRONİK MÜHENDİSLİĞİ

Bu tez 14/05/2019 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Dr. Öğr.Üyesi Mustafa Zahid YILDIZ Jüri Başkanı	Prof. Dr. İhsan PEHLİVAN Üye	Doç. Dr. Mehmet Recep BOZKURT Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Galip Çağan NASUHOĞLU
14/05/2019

TEŞEKKÜR

Yüksek lisans tez sürecimde bilgi ve deneyimleriyle bana yardımcı olan ve yönlendiren, değerli danışman hocam Dr. Öğr. Üyesi Mustafa Zahid YILDIZ'a teşekkürlerimi sunarım.

Tez konumu belirleme aşamamdan çalışmamı noktalayana kadar desteklerini esirgemeyen, değerli bilgileri ile beni aydınlatan Cem Gümüş'e çok teşekkür ederim.

Bu zorlu ve uzun süreçte beni anlayışla karşılayan, destek olan çok değerli arkadaşlarıma ve aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

AAA	: Açık anahtar altyapısı
DApp	: Dağıtık uygulama
ESHS	: Elektronik sertifika hizmet sağlayıcı
EVM	: Ethereum sanal makinesi
NES	: Nitelikli Elektronik Sertifika
OCSP	: Çevrimiçi sertifika durum protokolü
P2P	: Eşler arası
PoA	: Otorite ispatı (Proof of Authority)
PoS	: Varlık İspatı (Proof of Stake)
PoW	: İş İspatı (Proof of Work)
SİL	: Sertifika iptal listesi
SM	: Sertifika makamı
SPoF	: Tek nokta hatası
TK	: Telekomünikasyon Kurumu

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

BLOCKCHAIN TEKNOLOJİSİYLE AÇIK ANAHTAR ALTYAPISI TABANLI ELEKTRONİK SERTİFİKA DURUM BİLGİLERİNİN YÖNETİLMESİ

ÖZET

Güvenli bilgi alışverişi ve depolanmış verinin güvenliği için Açık Anahtar Altyapısı (AAA) bir yapıtaşı teknolojisidir. Açık anahtar sistemlerinde en yaygın kullanılan uygulamalardan bir tanesi elektronik imzadır. AAA kullanılarak oluşturulan elektronik imzaların elektronik ortamda gerçekleştirilen işlemlerde ıslak imza gibi hukuksal bağlayıcılığı bulunmaktadır. T.C. 5070 sayılı Elektronik İmza Kanunu'nda belirtildiği şekilde elektronik sertifika, elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik dosyalardır. Elektronik imza, Nitelikli Elektronik Sertifika (NES) kullanılarak oluşturulur. Sertifikalar X.509 standardına uygun olarak üretilir ve bu standartla uyumlu olan akıllı kartlara yüklenebilir.

Günümüzde geleneksel AAA sistemler, Sertifika Makamı (SM) tabanlı tek bir noktaya bağlı çalışarak bir merkeze güvenmeyi zorunlu hale getirmektedir. Geleneksel AAA sistemlerdeki elektronik sertifika iptal bilgilerinin kontrolü için yaygın olarak kullanılan iki yöntem bulunmaktadır. Bu yöntemlerden birincisi yetkili Elektronik Sertifika Hizmet Sağlayıcısı tarafından belirli periyotlarla yayınlanarak çevrimdışı çalışan Sertifika İptal Listesi (SİL)'dir. Diğer yöntem ise gerçek zamanlı sertifika durum sorgusu yapılabilen Çevrimiçi Sertifika Durum Protokolü (OCSP)'dür. Bu yöntemlerin hem ayrı ayrı hem de ortak sorunları mevcuttur.

Yüksek güvenlik gerektiren durumlarda çevrimiçi yöntemlerin kullanılması olası yanlış işlemlerin engellenmesi adına önemlidir. Bu çalışmada elektronik sertifika durum bilgilerinin bir X.509 hibrit sertifika yapısı kullanılarak blockchain platformu üzerinde tutulması önerilmektedir. Hibrit sertifikaya eklenen yeni alanlar, sertifika hiyerarşisi ve blockchainde ihtiyaç duyulacak bilgiler gözetilerek planlanmıştır. Çalışmada, AAA yapısındaki sertifikalandırma sürecine uygun olarak blockchain teknolojisinin entegre edilmesi için genel bir bakış açısı tasarlanmıştır. Kullanıcı arayüzü aracılığıyla sertifikaların durum bilgilerine sürekli ve kolay erişim sağlanabilecek blockchain ile etkileşimde bulunan bir prototip dağıtık uygulama geliştirilmiştir. Bu dağıtık uygulama ile hem sertifikaların anlık durum bilgilerine, hem de geçmişe dönük bilgilerine ulaşılabilmektedir.

Anahtar kelimeler: Açık anahtar altyapısı, kriptoloji, blockchain, ethereum, nitelikli elektronik sertifika, elektronik imza, sertifika durum bilgisi

MANAGEMENT OF ELECTRONIC CERTIFICATE STATUS INFORMATION BASED ON PUBLIC KEY INFRASTRUCTURE WITH BLOCKCHAIN TECHNOLOGY

SUMMARY

Public Key Infrastructure (PKI) is a milestone technology for safe information exchange and the security of stored data. One of the most commonly used applications in public key systems is electronic signature. Electronic signatures created by using PKI have legal binding as wet signature in electronic environment. Electronic certificate, which specified in the Republic of Turkey Electronic Signature Law No. 5070, is electronic files containing the data required for verification of electronic signature and identification information of the signatory. The electronic signature is created by using the Qualified Electronic Certificate (QEC). Certificates are produced in accordance with the X.509 certificate standard and can be installed on smart cards that are compatible with this standard.

Nowadays, traditional PKI systems rely on a single point based on the Certification Authority (CA), making it compulsory to rely on a center. There are two commonly used methods for controlling electronic certificate revocation information in conventional PKI systems. The first of these methods is the Certificate Revocation List (CRL) which works offline by being published periodically by the authorized Electronic Certificate Service Provider. The other method is the Online Certificate Status Protocol (OCSP), which can be used to query real-time certificate status. These methods have both separate and common problems.

In situations where high security is required, the use of online methods is important to prevent possible incorrect operations. In this study, it is recommended to keep electronic certificate status information on the blockchain platform using an X.509 hybrid certificate structure. The new fields added to the hybrid certificate are planned by taking into account the information needed in the certificate hierarchy and blockchain. In this study, a general perspective has been designed to integrate blockchain technology in accordance with the certification process in the structure of PKI. A distributed application prototype has been developed that interacts with the blockchain, which provides continuous and easy access to the status information of certificates through the graphical user interface. With this distributed application, both the instant status information of the certificates and the historical information can be accessed.

Keywords: Public key infrastructure, cryptology, blockchain, ethereum, qualified electronic certificate, electronic signature, certificate status information

BÖLÜM 1. GİRİŞ

İnsanlar yazının icadıyla başlayıp günümüze kadar haberleşmede farklı yöntemler kullanarak bilgi gizliliğine önem verdi. Günümüzde internet ve bilgisayar kullanımlarının artmasıyla beraber geleneksel iletişim yöntemleri yerini elektronik iletişime bırakmıştır. Bu değişimle beraber elektronik ortamda güvenlik ve özellikle siber güvenlik kavramı oldukça önem kazanmıştır. Bilgi sistemleri arasındaki haberleşmenin küresel boyutlarda yaygınlaşması olası birçok saldırıya karşı bilginin korunması konusunda önem arz etmektedir. Kriptografi, bilginin gizli tutularak istenmeyen taraflarca anlaşılmayacak bir hale dönüştürülmesini sağlayan tekniklerin bütünüdür. Gizlilik, bütünlük, inkar edememe gibi bilgi güvenliği kavramlarının sağlanması için matematiksel yöntemler kullanır. Kriptanaliz, şifrelenmiş anlamsız metinlerin çözümünü bulma yöntemidir. Kriptoloji ise kriptografi ve kriptanalizin bütününü kapsar. Kriptoloji, haberleşmede veri güvenliğini sağlayan kripto cihazları ile bu cihazlarda kullanılan algoritmaların güvenilirliğini araştıran elektrik ve elektronik mühendisliği, bilgisayar bilimleri, matematik, gibi disiplinler arası bir bilim dalıdır (Akleylek, Yıldırım ve Tok, 2011). Elektronik Mühendisi ve Matematikçi Claude Elwood Shannon'un 1949'da yayımlanan 'Gizlilik Sistemlerinin İletişim Teorisi' makalesi modern kriptografinin başlangıcı kabul edilir. 1970'li yıllara kadar askeri ve resmi kurumların tekelinde olan kriptografik yöntemler, 1976 yılında Diffie ve Hellman adlı iki araştırmacının önerdiği açık anahtarlı sistemler ile devrim geçirerek yeni bir boyut kazanmıştır. Açık anahtarlı sistemlerin keşfiyle beraber ortak gizli anahtarın bilinmeden de güvenli bir haberleşme sağlanabileceği ortaya çıkmıştır.

Blockchain teknolojisi ilk olarak 2008 yılında tanıtıldı. İlk uygulaması olan Bitcoin için 2009 yılında Satoshi Nakamoto takma adı kullanılarak eşler arası elektronik nakit sistemi bildirisi yayımlandı (Nakamoto, 2009). Bitcoin'in çıkmasından itibaren blockchain teknolojisinin müşterilere sağladığı kolaylık ve güvenilirlikle beraber kripto paraların popülerliği artmaya devam etmiştir. Blockchain teknolojisi, sahip olduğu

temel özellikler ile ön plana çıkmaktadır. İlk özellik, dağıtık yapısı sayesinde eşler arasında aynı defterin paylaşılarak tek nokta hatasının (SPoF) engellenmesidir. Bu özellik sayesinde tek bir noktaya güvenmeye gerek olmadan daha güvenilir ve sürekli bilgi alınabilmesi sağlanır. İkinci özellik, sadece yazmaya izin veren (append-only) yapısı sayesinde geçmiş verilerin değiştirilmesi engellenir. Bu özellik için kriptolojiden faydalanılır ve yüksek güvenlik özelliği sayesinde yüzyılın teknolojisi olarak gösterilmektedir. Üçüncü özellik, işlemlerin ağ üzerindeki düğümler arasındaki konsensüs algoritmaları ile yönetilmesi sayesinde üçüncü bir tarafa güvenmeye gerek duyulmaz. Bir bloğun zincire eklenmesi, düğümlerin çoğunun bloğu doğrulaması sonrasında gerçekleşmektedir. Son özellik olarak, blockchain şifreleme ve yetkilendirme işlemleri için asimetrik anahtarlar kullanır. Blockchain teknolojisinin en başarılı uygulamalarından bir tanesi de akıllı sözleşmelerdir. Akıllı sözleşmede önceden tanımlanan durumlar oluştuğunda otomatik olarak bu durum sonucunda yapılacak işlem gerçekleşir. Blockchain teknolojisi sağlık, kamu hizmetleri, finans, lojistik gibi birbirinden farklı alanlarda kullanılabilmektedir.

Blockchain teknolojisinin yapı taşlarından biri açık anahtar kriptolojidir. Blockchain teknolojisinde işlemlerin gizli anahtar ile imzalanması, hesap adreslerinin açık anahtar olarak kullanımı, gizli anahtar ile imzalanmış işlemlerin açık anahtarla doğrulanması gibi temel işlevlerde açık anahtar kriptolojisi kullanılmaktadır.

AAA, bir güvenlik altyapısını sağlamak için birlikte kullanılan yöntemler ve teknolojilerle beraber şifrelemeyi güvenli bir şekilde kullanmak için dijital sertifikaların oluşturulması, yönetilmesi, dağıtılması, kullanılması ve iptal edilmesi için gereken ilkeleri ve prosedürleri tanımlar. Açık anahtar sistemlerinde en yaygın kullanılan uygulamalardan bir tanesi elektronik imzadır. Elektronik imzalar oluşturulurken RSA, ECDSA gibi kullanılacak algoritmanın belirlenmesinden sonra hangi donanımlar ile kullanılacağı önemlidir. En çok bilinen ve kullanılan elektronik donanımlardan birisi akıllı kartlardır. Akıllı kartlar ile şifreleme, şifreleme çözme, imzalama, imza doğrulama ve anahtar depolama gibi özellikler sunulmaktadır. Akıllı kartların kullanılabilmesi için bilgisayar ile uyumlu kart okuyucular kullanılır (Akleylek ve diğerleri, 2011).

T.C. 5070 sayılı Elektronik İmza Kanunu'nda belirtildiği şekilde elektronik sertifika, elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik

bilgilerini içeren elektronik dosyalardır (Resmi Gazete, 2004). Aynı Kanunun 9 uncu maddesinde detayları belirtilen NES (Nitelikli Elektronik Sertifika) özetle, ESHS (Elektronik Sertifika Hizmet Sağlayıcı)'nin kimlik bilgileri ve kurulduğu ülke adını içeren, imza sahibinin kimliğinin tespitinin sağlanabildiği, sertifika geçerlilik süresinin başlangıç ve bitiş tarihini, sertifika seri numarası gibi bilgileri barındıran elektronik sertifikalardır (Resmi Gazete, 2004). NES'e dayanarak oluşturulan elektronik imzaların elektronik ortamda gerçekleştirilen işlemlerde ıslak imza gibi hukuksal bağlayıcılığı bulunmaktadır. Hızla dijitalleşmenin devam ettiği günümüzde sağlık, finans, lojistik gibi birbirinden farklı sektörlerde hizmet veren firmalar faaliyetlerini dijital ortama taşımış veya taşımaya devam etmektedir. Dijital verilere güvenin sağlanması açısından elektronik imza büyük önem teşkil etmektedir.

Elektronik sertifikaların birçok nedenden dolayı durum bilgisi değişebilir. Sertifikanın özel anahtarının kaybedilmesi, sertifika sahibinin bilgilerinin değişmesi, kullanıcının iptal talebi gibi farklı durumlarda sertifika iptal edilebilir. Bununla beraber belli bir süre kullanılmayacak olan sertifikanın askıya alınması, askıdaki sertifikanın tekrar geçerli duruma getirilmesi gibi sertifika durum değişikliği gerektirecek durumlar için de talepler sertifika hizmet sağlayıcıları tarafından karşılanır.

Geleneksel AAA sistemler SM tabanlıdır ve sertifikaların iptal bilgileri ilgili SM tarafından yayınlanır. Sertifikaların iptal bilgisi için en yaygın kullanım SM'lerin belirli aralıklarla SİL dosyaları yayınladığı ve/veya anlık OCSP cevaplarının aldığı yöntemlerdir (Başçi, 2008).

SSL/TLS sertifikaları, NES, kod imzalama sertifikaları, güvenlik sertifikaları gibi farklı tipte sertifikaların tamamı AAA teknolojilerine dayanan X.509 sertifikalardır. X.509 sertifika tabanlı olan SSL/TLS sertifikaları ve NES farklı amaçlara hizmet ederler. SSL/TLS sertifikaları genellikle veriyi kullanan sunucu kaynağının kimliğini doğrulamak için kullanılır. Diğer sertifikalardan farklı olarak NES'lerin sağlaması gereken özellikler RFC 3739 (Santesson, Polk ve Nystrom, 2004)'da ve bu teknolojiyi kullanan ülkeler tarafından NES özelinde çıkartılan elektronik imza kanunlarında detaylandırılmıştır. Bu çalışma X.509 v3 sertifika standartlarına göre elektronik imzalarda kullanılan NES özelinde hazırlanmıştır fakat diğer X.509 v3 sertifikalarında da kullanılabilir.

1.1. Çalışmanın Katkıları

Elektronik sertifika durum bilgilerinin izlenebilirliği ve yönetimi, hizmetlerin güvenilir bir şekilde sunulması için önemlidir. Bu önem açısından blockchain sahip olduğu özelliklerle sertifika durum bilgilerinin saklanması için uygun bir teknolojidir. Blockchain teknolojisinin yüksek erişilebilirlik, veri bütünlüğü ve hata toleransı özellikleri sayesinde tek nokta hatası (SPoF) engellenerek sertifika durum bilgilerine güvenilir ve sürekli erişim sağlanır. Ağ üzerindeki işlemlerin düğümler arasındaki konsensüs algoritmaları ile yönetilmesi sayesinde üçüncü bir tarafa güvenmeye gerek duyulmaz.

Bu çalışma X.509 v3 sertifika standartlarına göre elektronik imzalarda kullanılan NES özelinde hazırlanmıştır fakat diğer X.509 v3 sertifikalarında da kullanılabilir.
Çalışma özetle aşağıdaki katkılara sahiptir:

- Elektronik sertifikaların klasik SM tabanlı sertifika iptal kontrolü yapısına alternatif bir yöntem olarak blockchain yapısı kullanılarak sertifika durum kontrolü yapılabilecektir. Diğer bir ifade ile geleneksel sertifika durum bilgisi sorgulama yapısı korunurken blockchain ile alternatif bir yöntem sunulacaktır.
- Blockchain, merkezi veya dağıtık veri tabanlarına karşı sahip olduğu yüksek erişilebilirlik özelliği sayesinde merkeziyetçi yapıdan uzak olarak her zaman istenilen bilgiye ulaşım imkanı sunar. Elektronik sertifikaların durum bilgilerinin izlemesi ve yönetimi için hem güncel durum hem de geçmiş günlüklerine blockchain teknolojisi kullanılarak erişilmesi sağlanacaktır.
- Blockchain, sağladığı yüksek veri bütünlüğü özelliği sayesinde güvenilir bir yapı sunar. Blockchain'in dağıtık defter özelliği sayesinde ağ üzerindeki katılımcı SM düğümlerinin hepsinde zincirin bir kopyası tutulur. SM düğümleri arasındaki konsensüs algoritmaları ve zincir üzerinde herhangi bir değişiklik yapılmasına izin verilmemesi veri güvenliği açısından en önemli özelliklerdir. Bu özellikler sayesinde geriye dönük olarak sertifika durum bilgilerinde herhangi bir değişiklik yapılmasına izin verilmeyerek daha güvenilir bir yapı sunulacaktır.
- Bu çalışmada son kullanıcılar, sertifikaların güncel ve geriye dönük durum bilgilerine kolay bir şekilde erişerek sorgulama yapılabilecektir. Bu sorgulama

yöntemi ayrıca adli işlemler gibi yüksek güvenilirliğe ihtiyaç duyulan durumlarda da verimlilik sağlayabilir. Blockchain yapısı ile ilgili varlıklar tarafından sürekli güncel, güvenilir ve kullanıcıya kullanım kolaylığı sağlayan bir yapı üzerinden başka bir üçüncü kişiye ihtiyaç olmadan daha hızlı sorgulamalar gerçekleştirilebilecektir.

- Yaşanan güvenlik olayları, geleneksel AAA yapısında oldukça güvenilir kabul edilen SM'lerin varsayıldığı kadar güvenilir olmadıklarını göstermektedir. Önerilen yapıda, sistemde sorunlu bir alt SM fark edilirse, sertifika durum bilgisi yayınlaması için yetkisi alınarak sistemden izole edilebilecektir. Böyle bir durumda ilgili SM'nin geçmiş sertifika durum işlemlerine ait bilgiler silinmez ve veriler ağdaki diğer dağıtık defterlerde muhafaza edilmeye devam edilir.
- Çalışma için geliştirilen prototip dağıtık uygulamanın kullanıcı ön yüzü sayesinde akıllı sözleşmede programlanan iş akışlarının doğru kurgulandığı test edilebilecektir.
- Geçmiş bir zaman dilimi için sertifika iptal bilgisinin elde edilmesinde geleneksel yöntemlerin yetersiz kaldığı durumlarla karşılaşılabilir. Bu gibi durumlarda SM yetkilisinden destek istenir. Ulaşılmak istenilen bilgi için üçüncü bir kişiye ihtiyaç duyulması fazla iş gücü ihtiyacını beraberinde getirir. Sertifika iptal bilgilerine blockchain kullanılarak, üçüncü kişiye gerek olmadan ve güvenilir bir yöntem kullanılarak erişilebilecektir.

1.2. İlişkili Çalışmalar

Yaşanan güvenlik olayları SM'lerin varsayıldığı kadar güvenli olmadıklarını göstermektedir. SM'ler yanlış operasyonlar (Morton, 2013; Zusman, 2008), ihlal olayları (Comodo Security Solutions, 2011; Global Sign, 2011), hükümet zorlamaları (Eckersley, 2011; Soghoian ve Stamm, 2011) gibi nedenlerle hileli sertifikalar imzalayabilir. Merkeziyetçi sistemlerin getirdiği temel sorunlar için literatürde farklı çalışmalar mevcuttur. Diğer taraftan farklı ihtiyaçlar ve yapılar doğrultusunda verilerin blockchain teknolojisinin avantajlarından faydalanılarak yönetildiği çalışmalar da mevcuttur. AAA sistemlerinin genel sorunlarına çözüm için blockchain altyapısından faydalanılmış çalışmalara bu bölümde yer verilmiştir. Bu çalışmalar, X.509 elektronik sertifikalarının yönetimini kapsayan SSL/TLS sertifikalara odaklanan çalışmalardır.

SSL/TLS ve NES sertifikaları temelde X.509 sertifika yapısında olsalar da kullanım amaçları farklıdır ve bu nedenle farklı ihtiyaçlar doğurabilirler. NES, elektronik imza için kullanılır ve uyumlu akıllı kartlara yüklenebilir. Literatürde NES sertifikaları için bu çalışmanın kapsamında sağlanan özelliklere sahip benzer bir çalışma bulunamamıştır.

Google, gerçek zamanlı olarak takip edilebilen ve denetlenebilen bir açık altyapıya sahip olan Sertifika Şeffaflığı (Certificate Transparency) projesini hayata geçirdi (Laurie, Langley ve Kasper, 2013). Sertifika Şeffaflığı, SM'lerin yayınladığı sertifikalar için herhangi bir üçüncü parti uygulamaya güven duymaya gerek olmadan herkese açık bir şekilde denetlenebilirliği amaçlamaktadır. Sertifika Şeffaflığı, SM'lerin sertifika yayınlama sürecini değiştirir. Sertifika yayınlama sürecindeki bu değişiklik, izinsiz değişikliklere karşı korunan ve sadece ekleme yapılabilen sertifika şeffaflığı günlüklerine yazılmasını zorunlu hale getirmektedir. Günlüklerin tutulduğu veri tabanları Merkle ağacı yapısından faydalanılarak yalnızca ekleme yapılması özelliğine sahiptir. İlgilenen herkes bir SM tarafından verilen sertifika şeffaflığı günlüklerini inceleme imkanına sahiptir. Bu şekilde SM'lerin hesap verme zorunluluğu artar ve daha güvenilir bir sistem desteklenmiş olur. Sertifika Şeffaflığı yapısı mevcut SSL yapısına sertifika logları, sertifika denetleyicileri ve sertifika denetmenleri bileşenlerini ekler. Tüm bileşenler, SSL sertifikalandırma sisteminin denetimine ve kamu gözetiminde olmasına destek sağlar. Bunun daha ötesinde sertifika şeffaflığı için sadece yazılabilir kayıtların olduğuna dair özel bir mekanizma tasarlanmamış olup silinen ya da değiştirilen kayıtların doğrulanması bağımsız denetçilerin periyodik olarak doğrulamasına bağlıdır (Yüksel, 2018). Sertifika Şeffaflığı yapısında, SM tarafından bir sertifika yayınlanması için bir ön sertifika oluşturulur. Oluşturulan ön sertifika, sertifika şeffaflığı sunucuları günlüklerine gönderiler. Sonrasında ilgili sunucudan SM'ye sertifika için bir SCT (Signed Certificate Timestamp) değeri gönderilir. Bu işlem sonunda sertifika yayınlanır (Laurie ve diğerleri, 2013). Log tabanlı Sertifika Şeffaflığı yapısı, SM'lerin yanlış davranışlarını hızlı bir şekilde algılamak için sertifikaların izlenmesi ve denetlenmesi gibi açık bir yapı sağlarken günlük sunucularının güvenliği ve veri tutarlılığı göz ardı edilir.

TrustChain olarak adlandırılmış (Bralić, Kuleš ve Stančić, 2017) çalışmada blockchain teknolojisi kullanılarak dijital imzalı belgelerin uzun süreli korunması için bir model

sunulmuştur. Arşivlenecek elektronik imzalı belgelerin uzun süre geçerliliğini koruyabilmesinde önemli olan, imzanın bir kez geçerli bulunmasından yıllar sonra da geçerliliğinin doğrulanabilmesi ve korunabilmesidir. Dijital imzaların iki davranışı vardır. Birincisi, bir belgenin bütünlüğünü garanti ederler. Bunun anlamı zamanında dijital imza ile eşleşmiş belgelerin içeriğinin garanti edilmesidir. İkinci olarak, güvenilirliği garanti ederler. Dijital imzadan sertifika makamı kullanılarak belirli bir kişiye ya da kuruluşa ulaşılabilir. Bu şekilde belgelerin belirtilen sahibine ait olduğu ve bu belgenin yasal bir belge olarak kullanılabileceğinden emin olunur. Çoğu dijital sertifika iptal olur. Fakat ilgili SM'ye erişememe ya da SM'nin kullanım dışı olması gibi bir durumla karşılaşılabilir. Böyle bir durumda sertifikalarının doğrulanması mümkün değildir. Dijital imzanın belirli bir tarihte var olduğunu ve verinin bütünlüğü kanıtlamak için zaman damgası fonksiyonları kullanılabilir. Fakat bu hem bir kuruluşa güvenmeyi gerektirir hem de zamanla dijital imzanın kullandığı kriptografik algoritmaların ve zaman damgasının zayıflayarak kırılabilir hale gelmesine neden olacaktır. Bu çalışmada elektronik imzalı belgeler için belirtilen eksiklikleri iyileştirmek adına arşivleme kuruluşlarına güvenmeye gerek olmadan değiştirilemez ve herkes tarafından okunabilecek blockchainde depolanan dijital imzaların özetlerinin tutulduğu bir yapı önerilmiştir. Bu yapıya göre ilgili kişi veya kuruluşlar blockchaine bir kayıt eklenmesi için talepte bulunurken sadece yetkili düğümlerin blockchaine veri yazma hakkına sahip olduğu yarı açık bir sistem önerilmiştir. Yeni bir kayıt eklenmesini talep eden bir taraf ve düğümler arasındaki iletişimin özel bir TrustChain müşteri yazılımı veya düğümlerin kendi tarafından sağlanan bir web arayüzü ile gerçekleştirileceği belirtilmiştir. Blockchain'de veri boyutlarını arttırmamak adına belgelerin kendisi TrustChain sistemi dışında farklı bir noktada depolanırken sadece dijital imzalı belgenin özeti blockchain sisteminde tutulmaktadır. Yapıda, elektronik sertifikaların iptal kontrolü için geleneksel OCSP yönteminin kullanılması önerilmiştir. TrustChain düğümleri, TrustChain projesine katılan kurumlar tarafından tutulan sunuculardır. Bu sunucular yeni kayıt taleplerini kabul eder, bunları işler ve blockchaine yazarak ilgili tarafların okuması için ulaşılabilir halde tutar. Blockchain'e bir blok eklenirken düğümler Round Robin sistemi gibi davranır. Bir düğümün kendi sırası geldiğinde ilgili aday düğüm kayıtları toplar ve tüm imzaları doğrulamaya çalışır. Bir imza başarısız olursa, kayıt geçersiz sayılır ve yeni kayıtlar toplanır. Yeterli sayıda geçerli kayıt

bulunduğunda bir blok'a eklenirler. Fakat bu aşamada kayıtlar hala blockchaine kaydedilmemiş olurlar. Ekleme işlemi gerçekleşmeden önce, bütün kayıtların imza geçerliliğinin belirli bir sayıdaki diğer düğümler tarafından doğrulanması gerekmektedir. Tüm kayıtların imza geçerliliğini onaylamak için belirli sayıda başka düğümler gerekir. Blokun geçerli olduğu konusunda düğümlerin çoğunluğu hemfikir olursa blockchaine eklenebilir. Aksi takdirde, blok atılır ve bloku oluşturan kayıtlar yeni kayıt kuyruğuna döndürülür. Önerilen bu çözümde bilinen blockchain konsensüs konseptinden ziyade zaman damgası ve Round Robin yöntemleri ile blockchainin yönetilmesi önerilmiştir.

Sertifika iptal bilgilerinin sürekli olarak kullanılabilirliği ve güncellenmesi, çevrimiçi hizmetlerin güvenliğini sağlamanın önemi gözetilen çalışmada (Baldi ve diğerleri, 2017) elektronik sertifikaların yayınlanması ve doğrulanması için tüm sertifika bilgilerinin blockchain yapısında tutması planlanmıştır. Bu amaçla üç farklı rolden oluşan bir mimari tasarlanmıştır. İlk ve en önemlisi, gerekli koşulları sağlayan kullanıcılara sertifika yayınlayan ve sertifika iptal bilgilerinin devamlılığını sağlayan Sertifika Makamları (SM)'dır. İkinci rol olan servis sağlayıcıları (SP) kullanıcıların talep ettiği sertifika yayınlama istekleri için kullanılır. Üçüncü rol ise sertifikaları ve ilgili sertifika iptal bilgilerini okuyan kullanıcılardır. Bu tip bir yapının özel bir blockchain tipine dayalı bir altyapı kullanılarak gerçekleştirilebileceği belirtilmiştir. Önerilen yapıda sertifika doğrulama işlemi güncel SİL'in ortak dağıtık defterlerden okunması üzerinedir. SİL, sadece SM'ler tarafından yazılabilir. Bütün ağ kullanıcıları sertifika doğrulamak için SİL bilgisini herkese açık defterlerden okuyabilir. Önerilen şemayı uygulamak için açık kaynak kodlu özel bir blockchain platformu sağlayan ve PoW konsensüs algoritması kullanan Multichain yazılım aracı önerilmiştir. Her SM'nin kendine özel bir ID ile sertifika yayınladığı belirtilen çalışmada hangi SM'nin iptal bilgilerini yayınladığı bilgisine bu id numarası kullanılarak ulaşılabileceği belirtilmiştir. Fakat belirtilen işlemin nasıl yapılabileceği konusunda eksiklik mevcuttur. Bunun yanında blockchain kullanılarak kullanıcıların güncel SİL bilgisine ulaşmasına odaklanılmış fakat sertifika durum bilgileri tarihçesine erişim ihtiyacına değinilmemiştir.

Yakubov, Shbair, Wallbom, Sanda ve State (2018), çalışmalarında blockchain tabanlı bir AAA yönetim altyapısıyla X.509 sertifikalarının yayınlanması, doğrulanması ve

iptal edilmesini tasarlamışlardır. Çalışmada, X.509 sertifikalarının genişletilmiş alanına blockchainde kullanılacak bilgilerin gömülmesi sayesinde standart X.509 sertifikasının blockchain tabanlı AAA yaklaşımına uyumlu olması sağlanmıştır. Dijital sertifikaların güvenilir bir şekilde yönetilebildiği blockchain tabanlı bir PKI tasarlanarak uygulamaya alınmıştır. Çalışma kapsamında tasarlanan AAA yapısı restful servis, sertifika doğrulama ve kullanıcı arayüzü şeklinde üç ana başlık altında toplanmıştır. Restful servis kullanılarak ethereum açık ağına erişim sağlanmıştır. Bu servis sertifika yayınlama, iptal ve doğrulama işlevlerini sağlamaktadır. Sertifika doğrulama için akıllı sözleşmeden faydalanılmıştır. Kullanıcı arayüzünde ise tasarımın testleri gerçekleştirilmiştir. Sertifika doğrulama için hem ethereum akıllı sözleşme hem de Restful servisinin sağladığı sertifika doğrulaması performans açısından karşılaştırılmış ve ethereum Rinkeby test ağı kullanılarak akıllı sözleşme ile yapılan doğrulamanın daha etkili olduğu görülmüştür.

Blockchain tabanlı merkezi olmayan dijital sertifika yapısının anlatıldığı (Zhang ve Ma, 2018) çalışmada öne geçen özellik, blockchain teknolojisini sertifika iptal mekanizması ile birleştirerek SM'ler arasında dağıtılmış konsorsiyum blockchain tipinde hata toleransının düşük olduğu bir yapı oluşturmanın hedeflenmesidir. İkinci olarak, hatalı işlemlerde SM'ler için cezalandırma mekanizması mevcuttur. Yapıya göre seçilecek bir SM, diğer tüm SM'lerin taleplerini toplayarak bloğa yazar. Blok içerisinde kara listeye alınmış SM'ler de yer alırlar. Bloğun büyüklüğünü azaltmak için Merkle ağacı yardımıyla özet alınabileceği belirtilmiştir. Sonuç olarak sistemdeki SM'lerin işbirliği içerisinde olduğunu anlatan çalışma, SM'ler arasındaki konsorsiyum yapısına odaklanmıştır. Sistemde kullanıcıların bu sistemin neresinde olacağına ve baştan sona tüm sistemin nasıl yönetileceğine dair geniş bir bakış açısı yer almamaktadır. Ayrıca yapı sadece teorik olarak anlatımda kalmış ve uygulanabilirliğine dair bir çalışma yapılmamıştır.

CertChain (Chen ve diğerleri, 2018) çalışmasında TLS bağlantıları için blockchain tabanlı bir açık ve verimli denetim şeması öneriliyor. Özellikle, blockchain sisteminde güvenilirlik sıralaması tabanlı bir konsensüs protokolü ve sertifikanın ileri izlenebilirliğini desteklemek için yeni bir veri yapısı önerilmektedir. Ayrıca, alan tasarrufu için yanlış pozitiflerin ortadan kaldırılması ve sertifika iptal kontrolü için verimli sorgulama için DCBF (Dual Counting Bloom Filter) kullanan bir yöntem

sunulmuştur. Çalışmada muhasip (bookkeper) isimli sertifika işlemlerini açık denetim için blockchaine kaydeden yeni varlıklar tanıtılarak tanıtılmıştır. Blockchain tabanlı açık ve etkili denetim sistemi sunan TLS bağlantıları için CertChain önerilen çalışmada PoW, PoS veya DPoS gibi blockchaindeki en popüler ve yaygın olarak kullanılan konsensüs protokolleri yerine çalışmanın kendi modeli uygulanmıştır. Bu çalışmada müşteri, sunucu, SM'ler ve muhasipler olmak üzere 4 farklı varlık bulunmaktadır. Kullanıcı, sunucu ile TLS bağlantısı yapmak istemektedir. Sunucu, genellikle güvenli bağlantılar için SM'den sertifika almaya çalışan bir web sitesini belirtir. SM, geleneksel AAA'da sertifika imzalama ve yayınlamanın yanında sertifika işlemlerini imzalamak ve oluşturmaktan da sorumludur. Açık denetlenebilir servisi desteklemek için muhasipler, işlemleri bloklarda saklamak ve blockchaini koruma amacındadır. Blockchain, sadece yetkili düğümlerin sertifika yönetim sistemine katılım sağlayabildiği izne tabi sistemde çalışmaktadır. Sertifika iptal bilgilerinin daha efektif sorgulanmasına çözüm arayan bu çalışmada DCBF kullanılarak etkin veri depolama ve sorgulama işlemlerinde verimlilik sağlamıştır.

BÖLÜM 2. BLOCKCHAIN TEKNOLOJİSİ

Blockchain teknolojisi, Bitcoin ve Ethereum gibi kripto paraların kullandığı teknoloji olarak bilinmesine rağmen bu teknoloji sağladığı olanaklar ve çeşitlendirilebilir uygulamaları ile çok daha geniş bir kullanım alanına sahiptir. Temel olarak blockchain, değer içeren dijital ortamdaki verilerin açık ve güvenli bir şekilde depolanması ve yönetilmesine olanak sağlayan bir teknoloji olarak tanımlanabilir. Blockchain teknolojisi eşler arası ağlar (P2P), dağıtık veritabanları ve kriptoloji temellerine dayanmaktadır. Blockchain teknolojisinin getirdiği en önemli yenilik dağıtık ve ortak defter olmakla beraber bunun çok ötesinde esnek yeni bir teknolojidir. Bu teknolojinin sunduğu en önemli avantajlarından bir tanesi aracıları ortadan kaldırarak bilgi alışverişinde yüksek güvenlik sağlamasıdır. Blockchainin merkezi olmayan dağıtık yapısı sayesinde üçüncü bir kişiye ihtiyaç duymayarak sahteciliği ve hırsızlığı önlemesi bu teknolojiyi özellikle güvenliğin önemli olduğu sektörler için önemli hale getirmektedir. Sağladığı bu avantajlarla birbirinden farklı alanlarda kullanılabilir. Blockchain teknolojisinin kullanım alanları Şekil 2.1.'de gösterildiği gibi oldukça geniştir. Bu anlamda para transferleri, dijital kimlik işleri, akıllı sözleşme, doğrulama, şifreleme, oy verme, tedarik zinciri, ithalat, ihracat, sigorta, telif, askeri emir ve komuta gibi birbirinden farklı işler için kullanım olanağı sağlar.

Blockchain, güvenlik açısından iyi bilinen açık anahtar kriptolojisi, dijital imzalama ve özetleme gibi güvenlik uygulamalarını kullanır. İletişim açık/özel anahtarlar ile yapılır. Her düğüm topladığı işlemleri özel anahtarı ile imzalar. Ağdaki düğümler, IP adresleriyle değil açık adresleri ile adreslenirler. Blockchain teknolojisi, eşler arası ağlarda dağıtık defterlerle bir merkezi otoriteye ihtiyaç duymayan, sağlam algoritmik şifreleme ve doğrulama yöntemleri sayesinde yüksek güvenlik sağlayan bir teknolojidir.

Şekil 2.1. Blockchain kullanım alanı örnekleri

2.1. Eşler Arası (P2P) Ağlar

P2P ağların en önemli özelliği istemci ve sunucu yapısından farklı olarak her düğüm dağıtık bir iletişim modeli sağlamak için bir istemci ve aynı zamanda sunucu olarak çalışır (Bawa ve diğerleri, 2003). Eşler arası ağlardaki katılımcı düğümler eşit derecede ayrıcalıklıdır ve bir işlevi gerçekleştirmek veya bir hizmet sunmak için işbirliği yaparlar. 1999'da Napster gibi eşler arası ağlarda dosya paylaşımı yapılan ağlarla popülarite kazanmıştır (Carlsson ve Gustavsson, 2001). Ağdan herhangi bir cihazın düşmesi durumunda, ağ çalışmaya devam eder. Bu özelliği ile tek nokta hatası (SPoF) önlenmiş olur. Ayrıca indirme ve yükleme için çift yönlü kolay veri paylaşım olanağı sağlar.

2.1.1. Merkezi, Merkezi Olmayan ve Dağıtık Sistemler

Merkezi sistemlerde bilgi tek bir merkezde depolanır ve bilgiyi elinde tutan merkez onu değiştirme veya silme yetkisine sahiptir. Böyle tek merkezli bir yapının kontrol edilmesi ve yönetilmesi tek bir kontrol merkezi (single point of control) olduğundan kolaydır. Ancak merkezde yaşanan bir sorun tüm sistemi etkiler. Dolayısıyla sistemi etkileyebilecek hata noktası da bir tanedir (Montresor, 2008). Bir sertifika makamı ve yayınladığı sertifikalardan oluşan bir yapı merkezi bir yapıyı temsil etmektedir. Bu yapıda sistem tasarımcılarının değişken müşteri ve sunucu sayısını yönetmek için

sistemin ölçeklenebilir olup olmadığını hesaplamak adına ciddi hesaplamalar yapmalarını gerektirmektedir.

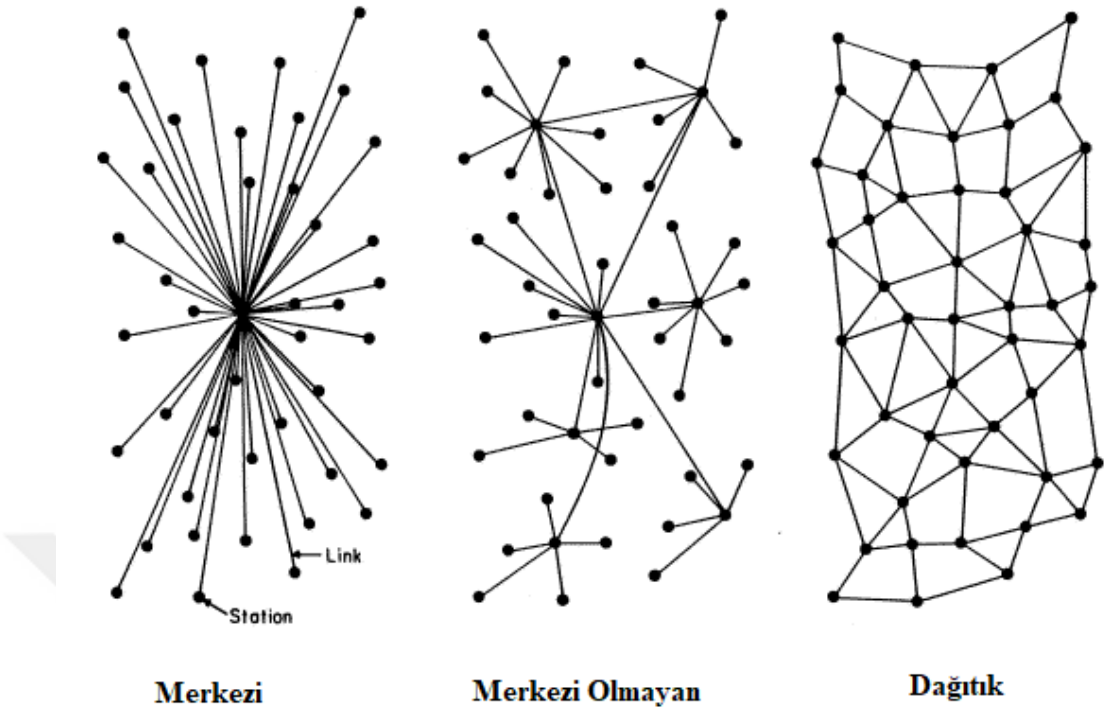
Merkezi olmayan sistemler, birden fazla küçük merkezi sistemin birbirine bağlanmasıyla oluşur. Sistemin tümü göz önüne alındığında tek bir merkezden söz edilemeyen ve fikir birliğinin tek bir merkezde yapılmadığı yapılardır. Bu açıdan merkezi ve dağıtık sistemlerin arasında kalmıştır.

Dağıtık sistemler merkezi sistemlere kıyasla hataya dayanıklı ve ölçeklenebilir sistemlerdir. Merkezileşmenin getirdiği sorunlar nedeniyle, eşler arası çözümlerin popülerliği her geçen gün artmaktadır. Şekil 2.2. üç farklı sistem modelini göstermektedir.

Diğer taraftan tek merkezli bir yapıya sahip olunmadığı için oluşturulması zordur. Araştırmalar P2P ağlar için aşağıdaki zorluklardan bahsetmektedir (Ali, 2017):

- Ölçeklenebilirlik: Dağıtık sistemler kaynak kullanımına göre sistemin verimli çalışmasına devam etmesini sağlamalıdır.
- Performans: Belli sistem yoğunluklarına göre dağıtık sistemlerin alacağı aksiyonların planlanmış olması önemlidir.
- Güvenilirlik: Aynı veri kaynağına erişen sistemlerin aynı veri sonuçlarına ulaşarak uyumlu ve tutarlı çalışması önemlidir.
- Önemsiz Veri Yazma: Bazı hız sınırlayıcı veya erişim kontrol mekanizması olmadan, P2P ağların eklenen veri miktarını sınırlandırma imkanı yoktur. Kötü niyetli olarak ağa çok fazla çöp verisi aktarılabilir ve düğümleri devre dışı bırakabilir.
- Eclipse Saldırısı: P2P ağın kontrolünün ele geçirilmeye çalışıldığı bir saldırıdır. Blockchain açısından düşünüldüğünde ağda kurban düşman tarafından kuşatılıp ağın geri kalanından izole edilir.

Dağıtık sistem yaklaşımı ile blockchain sisteminin dağıtık kayıt defterleri ortaya çıkmıştır. Blockchain, dağıtık eşler arası ağ üzerinde çalışmaktadır.



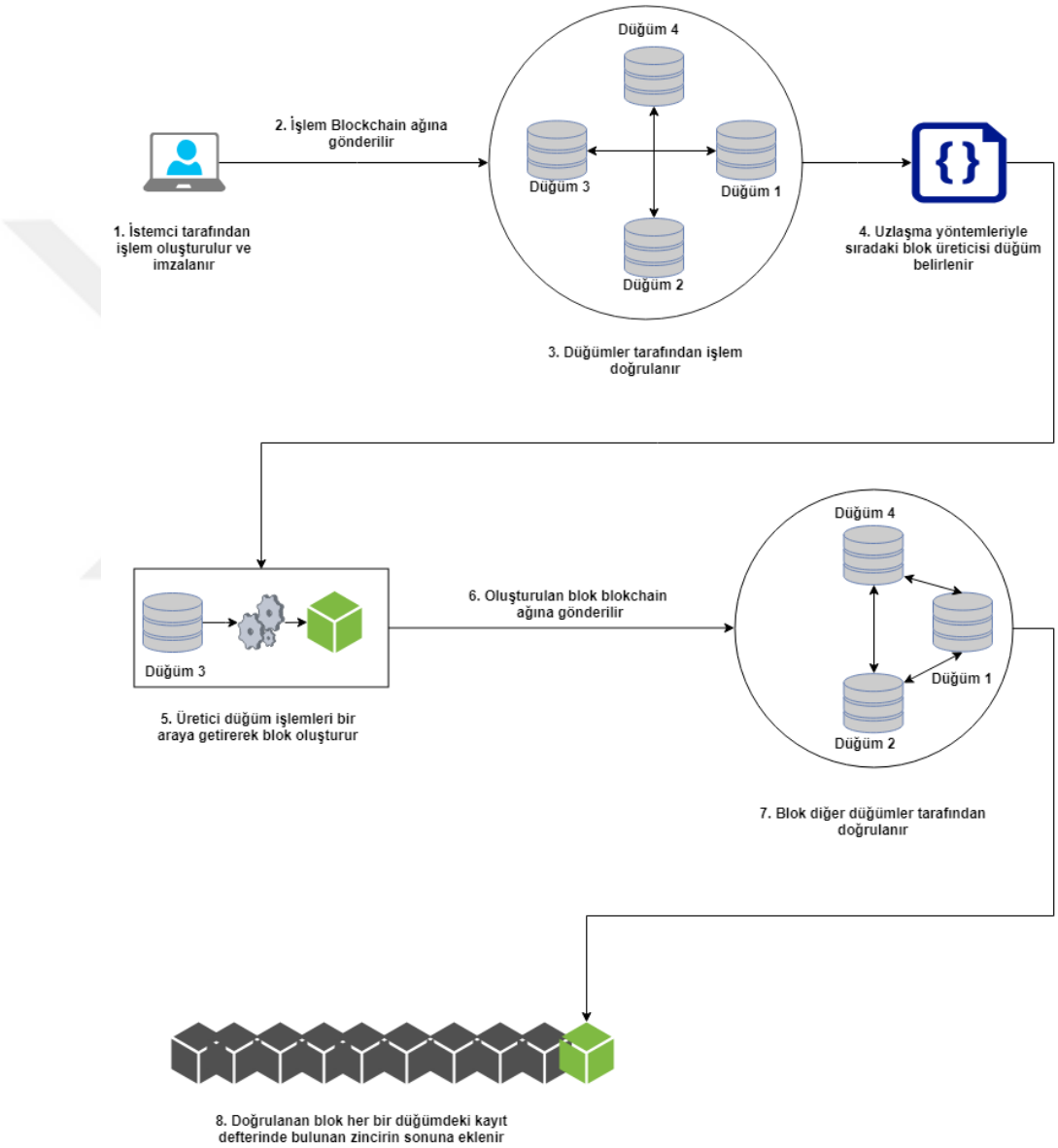
Şekil 2.2. Merkezi, merkezi olmayan ve dağıtık sistemler

2.2. Blockchain Temelleri

Blockchain, P2P ağlarda birbirine bağlı ve merkezi olmayan bir sistemde amacına uygun yazılımlar aracılığıyla çalışır. Bunun anlamı istemcinin merkezi bir sunucu yerine bir düğüme bağlanmasıdır. Blockchain teknolojisinde her bir düğüm, ağdaki tüm kayıtların bir kopyasını tutar. Bloklardaki herhangi bir verinin değiştirilmesi özetlerin değişmesine yol açacağından yapılan değişiklik kolaylıkla fark edilir. Sistemdeki düğümlerin doğrulama yapabildiği dağıtık defterlerle bir merkeze güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir.

En temel seviyede blockchain sisteminde işlem yapmak isteyen istemci bir özel anahtar ve ona bağlı bir açık anahtara sahip olmalıdır. Özel anahtarla imzalanan işlem P2P ağda yayınlanır. Bu yayınlama işlemi sadece alıcıya değil tüm ağa duyurulmak üzere bağlantıda olunan tüm düğümlere gönderilir. Ağda kurulan tüm iletişimde gönderici ve alıcıyı güvenli biçimde tanımlamak için kriptografiden faydalanılır. Gönderilen doğrulanmamış işlem, doğrulanmamış işlemler havuzunda doğrulanmak üzere bekletilir. Mesajı ilk kez alan düğümler işlemlerin kurallara uygun ve geçerli olduğunu

denetler. Bir bloğun hangi düğüm tarafından yayınlanacağı uzlaşma (konsensüs) yöntemleriyle belirlenir. Yayıncı düğümün ürettiği blok bağlı olduğu diğer düğümlere iletilerek doğrulanır. Doğrulama sonrasında blok, dağıtık kayıt defterlerindeki zincirinin son halkası olarak blockchaine eklenir. Blockchain mimarisi Şekil 2.3.'de gösterilmektedir.



Şekil 2.3. Blockchain mimarisi (Murat, 2018)

Sistemin temel özellikleri (Karaaslan ve Akbas, 2017):

- İşlemler merkezi değildir.
- İşlemler her kullanıcının belirli kurallar dahilinde eşit ve özgür olduğu P2P ağda tüm düğümlere yayınlanır. Tüm işlemler şeffaflıkla izlenebilir.
- İşlemler, düğümler tarafından onaylandıktan sonra blockchaine eklenebilir.
- Sistemdeki bütün hesaplar açıktır fakat anonimdir. Hesap ID aynı zamanda açık anahtardır.
- Madenci düğümler, işlem havuzlarındaki işlemleri doğrulayarak bloklar olarak blockchaine kaydeder.

2.3. Blockchain Temel Bileşenleri

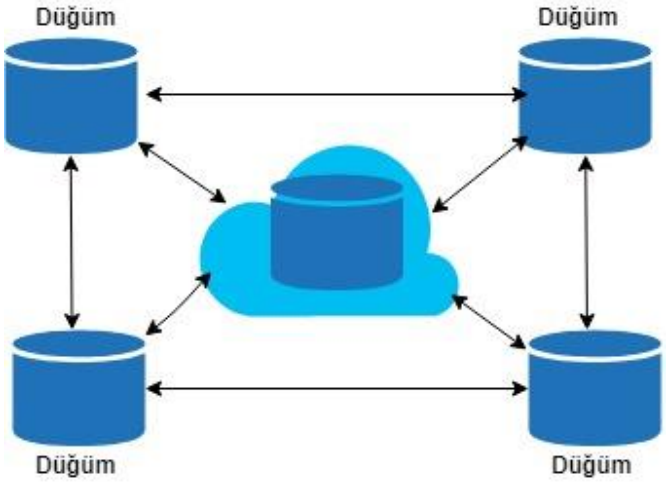
Blockchain sistemi, dağıtık veri yapısında üçüncü bir tarafa ihtiyaç olmadan katılımcılar tarafından doğrulanan blokların birbiriyle ilişkili bir şekilde art arda sıralı bir şekilde eklenmesiyle bir zincirin oluşturulduğu prensibe dayanır. Bu yapıdaki bileşenler dağıtık defterler, blok yapısı ve doğrulama mekanizması olarak sınıflandırılabilir (Kaya, 2018).

Blockchaindeki kayıt bütünlüğü açık anahtar kriptoloji iletişimi sayesinde gerçekleştirilir ve blok oluşumunda ve işlem kaydetmede özetlemenin yoğun kullanımı ile güçlendirilir (Bozic, Pujolle ve Secci, 2016).

2.3.1. Dağıtık Defterler

Blockchain, dağıtık defter teknolojisinin özel bir tipidir. Dağıtık defter teknolojisinde farklı kayıt sistemleri yerine tek bir kayıt sistemi vardır. İşlemler ortak olan bu deftere yazılır. Tek olan ortak defter değiştirilemez ve defterde geriye dönük bir değişiklik yapılamaz (Kaya, 2018). Tek ve dağıtık olan bu defterin bir kopyası blockchain ağındaki katılımcı tüm düğümlerde bulunur. Diğer bir ifade ile blockchain, ağdaki katılımcı düğümlerin hepsinin kendi veritabanı kopyasının olduğu düğümler tarafından yönetilir. Bir düğüm blockchain ağının korunmasında önemlidir ve ağa gönderilen işlemleri işlemede görev alır. Ağa yeni bir düğüm katılırsa blockchainin bir kopyasını edinir. Bir düğüm ağa bağlı bir bilgisayar, bir sunucu gibi elektronik bir cihaz olabilir. Blockchain'de tüm işlemler bloklar üzerinde şifrelenmiş olarak dağıtık defterlerde herhangi bir üçüncü tarafın onaylamasına gerek olmadan tutulur. Böyle bir yapıda bir

katılımcı düğüm üzerindeki kayıtlarda bir değişiklik olursa bloğun özet bilgisi değişeceği için değişiklik kolay bir şekilde tespit edilir. Blockchain'in teknolojisinin sahip olduğu en önemli özellikler dağıtık ve ortak defterlerdir. Şekil 2.4'de dağıtık defter yapısı yer almaktadır. Düğümler yapılarına göre basit düğüm, tam düğüm, madenci düğüm ve madenci havuzu olarak farklılık gösterirler (Kardaş, 2018).



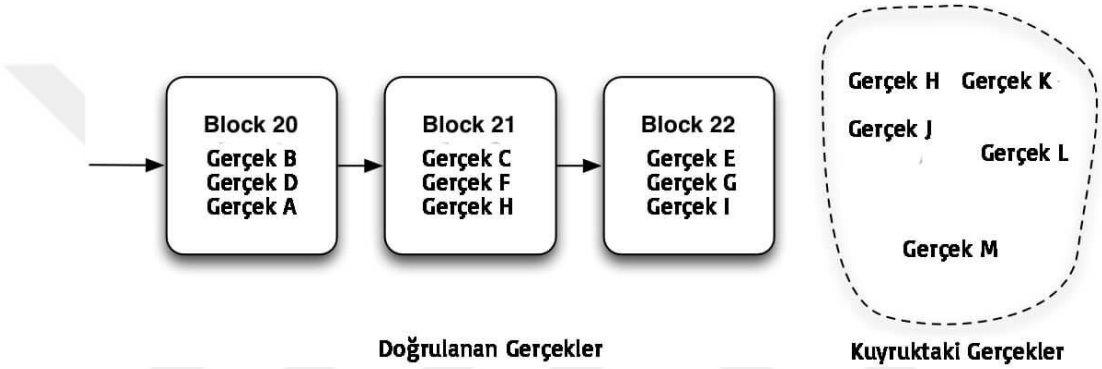
Şekil 2.4. Dağıtık defterler

2.3.2. Blok Yapısı

Blockchain teknolojisinde kriptografik fonksiyonlardan yoğun bir şekilde yararlanılır. Bunlardan bir tanesi olan özetleme fonksiyonları blockchain yapısında da aktif olarak kullanılmaktadır. Her blok bir önceki bloğun özet bilgisini tutar. Özet fonksiyonları olarak SHA-1, SHA-2, SHA-3, MD5, BLAKE gibi birçok farklı algoritma kullanılmakla beraber blockchain teknolojisi içerisindeki süreçlerde ihtiyaç duyulan kısımlarda SHA-2 algoritmasının bir alt kolu olan SHA-256 özetleme algoritması kullanılmaktadır (Murat, 2018). SHA-256 fonksiyonu, girdiler için 256 bitlik çıktılar üretir. 256 bitlik bir çıktı ise 2^{256} farklı fonksiyon çıktısı üretilebildiğini gösterir. Böyle bir çıktı değerinde çakışma olabilmesi için güncel bilgisayarların işlemci kapasiteleriyle imkansız olan en az 2^{128} deneme yapılmasını gerektirmektedir. Blockchain, her biri birbiriyle ilişkili bloklardan oluşmaktadır. Her bloğun başlık kısmındaki bilgiler SHA-256 algoritmasıyla özetlenerek bir sonraki blokta tutulur (Murat, 2018). Bu şekilde birbiriyle ilişkili blokların değiştirilmesi engellenir ve özet verilerinde yapılacak küçük

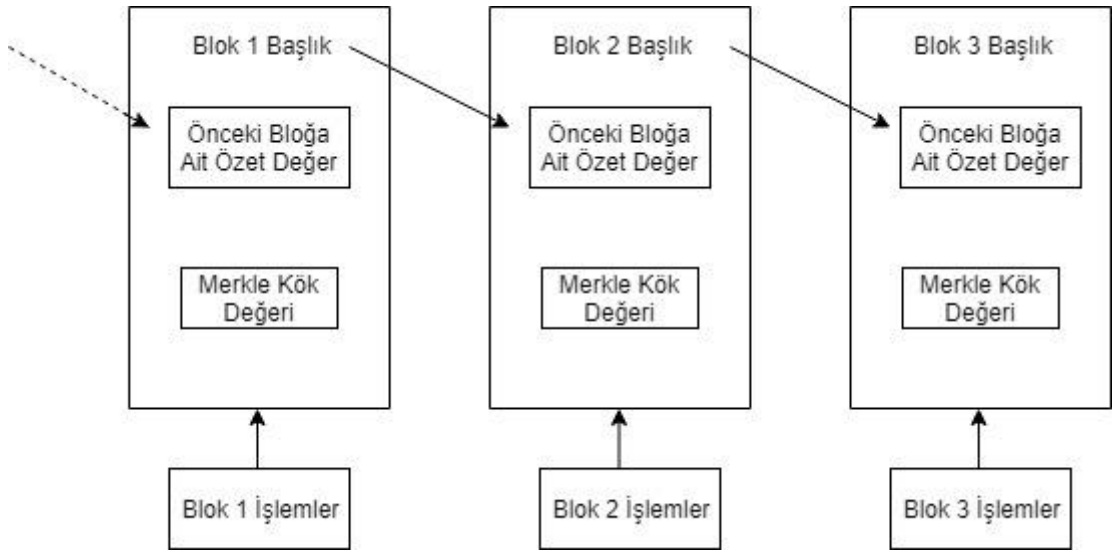
bir değişiklik özet değerini değiştirdiği için kolaylıkla fark edilir. Zincirin başlangıcı olan ve herhangi bir bloğa bağlı olmadan oluşan blok, genesis blok olarak adlandırılır.

Yetkili varlıklar tarafından gönderilen doğrulanmamış gerçekler, doğrulanmamış gerçekler havuzunda doğrulanmak üzere kuyrukta bekletilir. Gerçekler parasal işlemler, bilgi, işlem, olay, imza vb. şeyler olabilir. Örneğin Şekil 2.5.'teki gibi F gerçeği (bilgi, işlem, olay vb.) 21. blokta ve E gerçeği 22. blokta buluyorsa, E gerçeğinin tüm ağ tarafından F isimli gerçekten sonra geldiği düşünülür. Ayrıca bir bloğa ekleme yapılma esnasında, gerçekler doğrulanmamış olarak kuyrukta bekler.



Şekil 2.5. Doğrulanmış bloklar ve kuyrukta bekleyen gerçekler

Ağ üzerinde güvenilmeyen işlemlerin devre dışı bırakılması amacıyla bloklar kullanılır. Düğümler, kuyrukta bekleyen gerçeklerin ağ tarafından kabul edilen kurallara göre geçerli olup olmadığı belirlemek için analiz eder. Geçerli işlemler birlikte gruplandırılarak bir blok oluşturulur. Blockchain'e eklenen bir blok bir önceki blokla ilişkilidir yani her bir blok bir sonraki bloğa referans olur (Mendi ve Çabuk, 2018). Bu şekilde ilk bloktan son bloğa kadar zincirin tüm blokları birbirine bağlanış olur. Blokların birbiri ile ilişkisi Şekil 2.6.'da yer almaktadır.



Şekil 2.6. Blockchaini oluşturan bloklar

2.3.3. Blockchain Konsensüs

Blockchain'in P2P ağlarında bütünlüğün sağlanması ve düğümlerin birbirlerinden haberdar olması için konsensüs yani fikir birliği denilen uzlaşma sistemi kullanılır. İşlemlerin deftere işlenmesi ve aynı olması fikir birliği olarak isimlendirilen algoritmalar ile gerçekleştirilir. Bu yapıda tek merkezli yapıların aksine hak ve sorumluluklar sistemdeki aktörlere dağıtılmıştır. Teorik olarak ağdaki tüm aktörler bütün işlemleri onaylayabilir, reddedebilir, denetleyebilir ve işlemlerin tarihçelerini tutabilir. Bu nedenle sistem aktörleri arasında mutabakatın sağlıklı işlemesi son derece kritik bir öneme sahiptir. Farklı fikir birliği algoritmalarının farklı avantaj ve dezavantajları vardır. En popüler konsensüsler Bitcoin'de kullanılan ve madenciler (miner) arasında yapılan emek kanıtı (Proof of Work - PoW) algoritması ve Ethereum'da kullanılan hisse kanıtı (Proof of Stake - PoS) algoritmalarıdır (Kaya, 2018). Bu algoritmalar dışında pratik bizans hata toleransı (PBFT), delege edilmiş hisse kanıtı (DPoS), otorite ispatı (Proof of Authority - PoA) gibi farklı konsensüs algoritmaları mevcut olup yeni algoritmalar geliştirilmeye devam edilmektedir. Konsensüs seçimi farklı ihtiyaçlara ve farklı blockchain teknolojilerine göre değişmektedir.

2.3.3.1. İş Kanıtı (Proof of Work – PoW) Uzlaşma Yöntemi

İş kanıtı konsensüsü, Bitcoin'de kullanılan ve aynı zamanda Nakamoto konsensüs olarak da isimlendirilen bir algoritmadır. Bu yapıda madenciler (miner) olarak isimlendirilen makineler sistemin blok yapısını hazırlayıp, ilgili blockchain ağına eklenmesi için bir problemin çözümü üzerinde çalışırlar. Bir sonraki blok lideri, bulmacayı ilk çözen makinedir. Bulmaca, kriptografide trapdoor fonksiyonu olarak adlandırılan çözülmesi zor ancak doğrulanması kolay bir yöntem kullanılarak inşa edilmiştir.

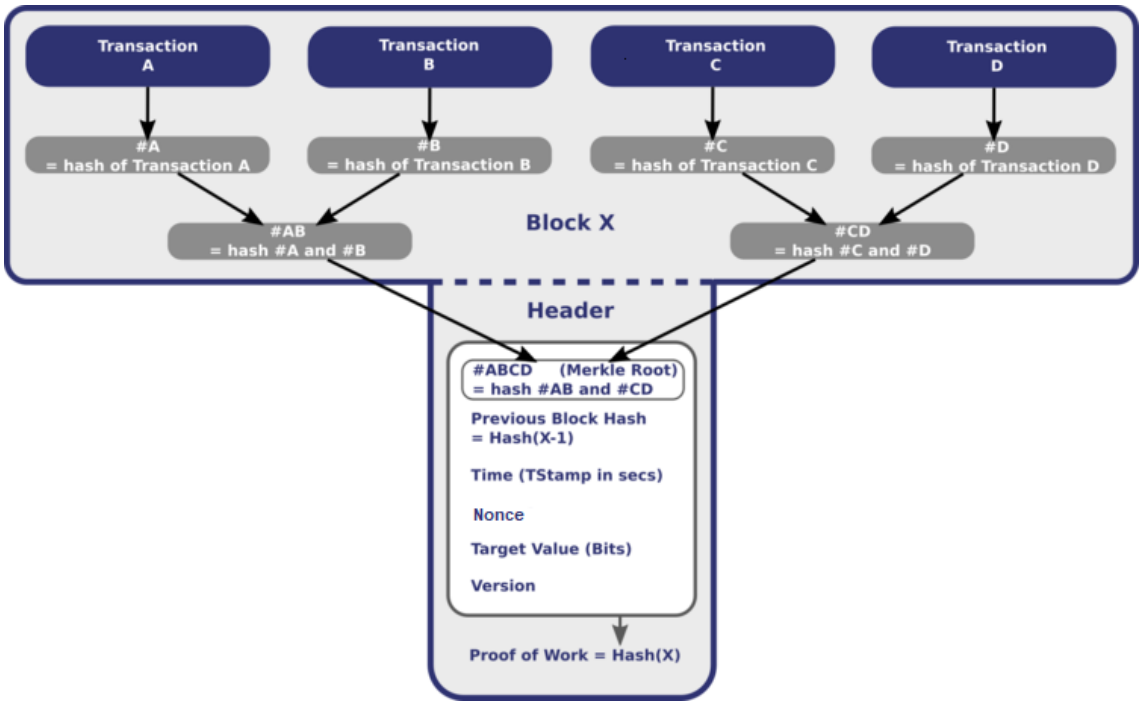
Emek kanıtı algoritmasındaki amaç madenciler arasında bir konsensüs oluşturarak işlemin deftere yazılması için el sıkışmaktır. Madenciler, mümkün olduğunca çok işlemi içeren fakat belirli bir büyüklüğü aşmayan bir blok oluşturmak için yarışırlar. Fakat bir blok bazı kurallara uygun şekilde oluşturulmalıdır. Kurallara uygun bir blok oluşturulabilmesi için madenciler çözülmesi zor bir problemi çözmeye çalışırlar. Bu problem, ağdaki düğümlerin değişiklik önerisi hakkı kazanmadan önce çözmesi gereken bir bulmaca gibidir. Problemi çözerek uygun bloğu bulan ilk madenci bitcoin ile ödüllendirilir. Madencilerin problemi çözerek bir blok oluşturabilmesi için çok hızlı deneme yanılma yapmaları gerekir ve bunun için de ciddi bir hesaplama gücüne ihtiyaç duyulur.

Bir blok temel olarak bir blok başlığı ve işlemler listesinden oluşur. Bir blok başlığının yapısı Tablo 2.1.'de yer almaktadır. Bir bloğun dijital parmak izi olarak ifade edilebilecek birincil tanımlayıcısı, blok başlığının iki kere SHA 256 algoritmasıyla özetinin alınmasından oluşur. Elde edilen 32 byte'lık özet değeri blok özeti olarak adlandırılır. Bir blok özeti tek bir bloğu temsil eder. Blok başlığındaki bilgilerden zorluk derecesi, nonce değeri ve zaman damgası madencilikle ilgilidir. Bir blokta, ortalama işlem boyutu 250 byte civarında olan 500'den fazla işlem yer alır. Blok başlığı ise 80 byte veri içerir (Antonopoulos, 2014).

Tablo 2.1. Blok başlığı yapısı

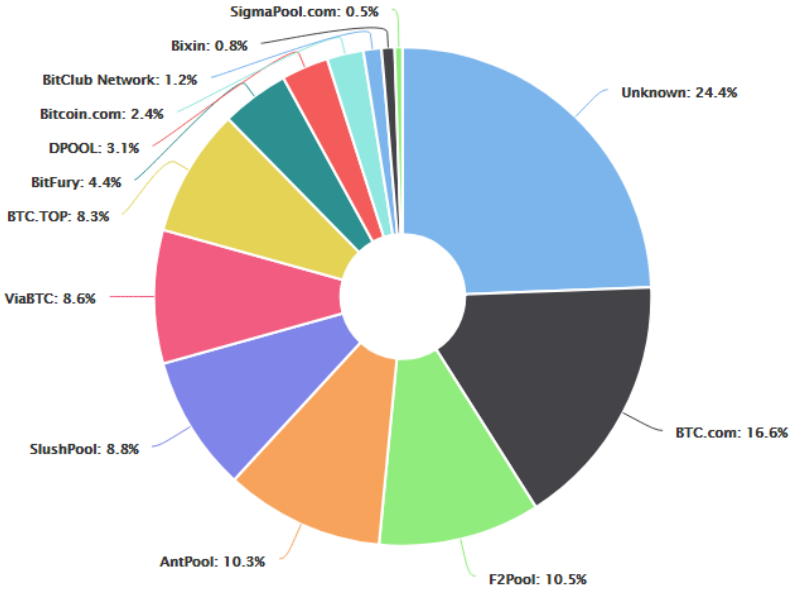
Alan	Açıklama	Boyut (Bytes)
Versiyon	Blok sürüm numarası	4
Zaman damgası	Bloğun oluşturulma zamanı	4
Zorluk derecesi	Emek İspatı algoritması zorluk hedefi	4
Önceki blok özeti	Referans edilen önceki bloğun özet değeri	32
Merkle Ağacı	Bloğun içerisindeki tüm işlemleri temsil eden Merkle ağacı özet değeri	32
Nonce	İş kanıtı işleminde kullanılan değer (sayaç)	4

Bloktaki tüm işlemlerin özet değerinin blok başlığında yer alması yerine Merkle ağacı kullanılarak bloktaki işlemlerin kombine edilmesi sonucunda tek bir özeti değeri elde edilir. En yaygın özet alma kullanımı ikili sistemdir. Bu yapıya göre verilerin sıralı şekilde özet bilgileri tutulur. Her bir veri, özet fonksiyonundan geçerek kendi özet fonksiyonlarını oluşturur. Bu özet fonksiyonları ikili şekilde yeniden bir özet fonksiyonuna sokularak yeni bir özet bilgisi elde edilir. En son tek bir özet bilgisi elde edilinceye kadar özet alınmaya devam edilir. Şekil 2.7.'de A,B,C,D olarak gösterilen dört farklı işlemin özetleri alınarak blok başlığında tek bir özet olarak yer alma işlemi gösterilmektedir.



Şekil 2.7. İş kanıtı (PoW) algoritması blok başlığı (Kehrli, 2016)

PoW konsensüs algoritmasında problemlerin çözümü yüksek miktarda enerji tüketimine neden olmakta ve özel donanım gereksinimleri ortaya çıkarabilmektedir. 2014 yılında yapılan bir çalışmada tüm Bitcoin ağının elektrik tüketiminin İrlanda ile eşit olduğunun tahmin edildiği belirtilmiştir (Malone ve O'Dwyer, 2014). Sadece yeni bloğu çözen ilk madenciye ödül verilen yapıda en yüksek işlemci gücüne sahip madencilerin ödülü alma ihtimali daha yüksektir. Bu yapı madencilik işlemlerinin kurumsallaşmasına ve büyük madencilik çiftliklerinin kurulmasına yol açmıştır (Mendi ve Çabuk, 2018). Ağda kötü niyetli düğümler ağın yarısından fazlasına sahip olmadığı müddetçe ortaya bir problem çıkmaz (%51 saldırısı). Şekil 2.8. bitcoin madenci havuzunun dağılımını göstermektedir. Bu şekilde işlem gücünün 50%'den fazlasını 3 tane madencilik havuzunun yönettiği görülmektedir. Bu yapı blockchainin temelini oluşturan merkezi otoritenin dağıtılması özelliğine zıt bir durumdur.



Şekil 2.8. Bitcoin madenci havuzu ("Bitcoin Hashrate Distribution", 2019)

2.3.3.2. Varlık İspatı (Proof of Stake – PoS) Uzlaşma Yöntemi

Varlık ispatı yönteminde blok yaratma koşulu işlemi katılımcıların cüzdan hesabındaki hisselere bağlı olarak yapılır. Madenciler ağa dahil olurken belirli bir süre harcayamayacakları istedikleri kadar bir kripto parayı riske atarak hisse satın alırlar. Bir blok oluşturarak ödülün alınması katılımcıların sistemdeki hisseleriyle doğru orantılıdır.

Sistemde yüksek miktarda hisse bulunduran katılımcıların doğrulayıcı olarak kullanılma olasılığı daha yüksektir. Bu sistemde daha çok hissesi olan katılımcıların sisteme saldırı yapma oranının düşük olduğuna inanılır. Tüm hisselerin %x payına sahip bir hissedar, %x olasılığı ile yeni bir blok oluşturur. Buna bağlı olarak bloğu oluşturacak katılımcı, sahip olduğu hisse pay oranına göre rasgele olmayan bir yöntemle seçilir.

Varlık ispatı yöntemi de iş kanıtı yönteminde olduğu gibi bir problemin çözülmesine ihtiyaç olmadığı için yüksek işlemci gücü gerektirmez ve gereksiz elektrik tüketimine yol açmaz. Katılımcıların sahip oldukları hisseleri ile alacakları ödül doğru orantılı olduğu için katılımcıları daha fazla yatırım yapmaya teşvik eder.

2.3.3.3. Otorite İspatı (Proof of Authority - PoA) Uzlaşma Yöntemi

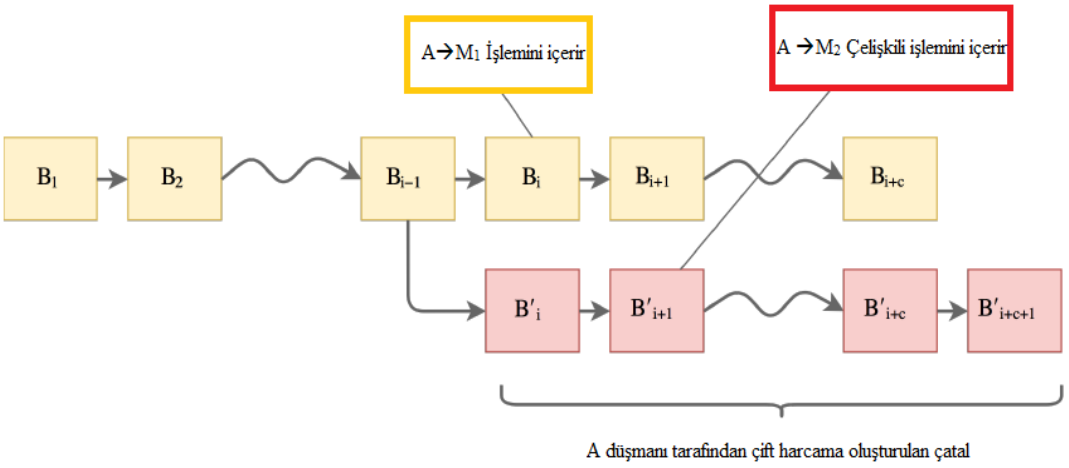
Her blockchain düğümü bütün zincirin kaydını tuttuğu açık blockchain modellerinde ölçeklenebilirlik sorunu mevcuttur. PoA, saniye başına daha fazla işlem yapabilme özelliği ile PoW ve PoS yöntemlerine göre daha ölçeklenebilirdir. PoA, madencilik gerektirmez. PoA mutabakat algoritmasında bir onaylayıcı olabilmek için dijital kimlikler kullanılır. Otoritelerin kimlikleri açıktır, anonim değildir. Otorite olmak için kimliklerin gerçek olduğunun ispatı gibi bazı şartların sağlanması gerekmektedir ve uygulanan prosedürler herkes için aynı olmalıdır. PoA mutabakat algoritmasındaki doğrulayıcı düğüm sayısı sınırlı sayıda olduğu için bu özelliği onu daha ölçeklendirilebilir bir sistem yapar. Kimlikleri açık ve saygınlığı olan düğümler özelliği ile daha çok özel blockchain ağlarına uygundur. PoA, bilgi gizliliğinin önemli olduğu kurumların özel bir ağda blockchain teknolojisinden faydalanmalarına imkan sağlar. Örneğin Ethereum Rinkeby test ağı, Microsoft Azure PoA algoritmasını kullanmaktadır.

2.4. Blockchain Güvenliği

Blockchain teknolojisinin sunduğu önemli avantajlardan birisi de güvenlik konusudur. Blockchain dağıtık defterlerine bir kayıt eklendikten ve ağda yayınlandıktan sonra kayıtlar geriye dönük olarak değiştirilemez. Her blok kendinden önce gelen bloğa bağlı olduğu için blokta yapılacak herhangi bir değişiklik ilgili bloğun özet değerini etkiler. Değişiklik sonucunda zincir bütünlüğü kaybolacak yani bir sonraki blok, değişikliğe

uğramış bloğu adreslemiyor olacaktır. Bu durumda zincirdeki bütünlük kaybolacağı için ağdaki kullanıcılar tarafından onaylanmayacaktır (Mendi ve Çabuk, 2018).

Finansal işlemlerde kullanılan blockchain, çift harcama problemi olarak da bilinen saldırılara izin vermez. Diğer bir ifade ile örneğin farklı iki eşyanın aynı para ile alınması engellenecek şekilde tasarlanmıştır. Bu atağı gerçekleştirebilmek için A isimli düşman ana zincirde bir çatal oluşturarak ağın bunu kabul etmesini sağlamalıdır. Örneğin M isimli müşterinin c onayını almayı beklediğini kabul edelim. Ürün gönderildikten sonra paranın A'dan M'ye gittiğini gösteren B_i işlemini içeren blockchain şu şekildedir: $B_1,B_2,\ldots B_i,B_{i+1},B_{i+2\ldots}B_{i+c}$. Bu işlemde zorluk derecesi k'nın bütün bloklarda aynı olduğu kabul edilerek, çatal oluşturmak isteyen düşman c′>c olacak şekilde $B_1,B_2,\ldots B'_i,B'_{i+1},B_{i+2\ldots}B'_{i+c'}$ bir çatal oluşturur. Bu çatal ağa dağıtıldığı zaman en uzun blok olarak ana zincir kabul edilir. Bu senaryonun gösterimi Şekil 2.9.'da yer almaktadır.



Şekil 2.9. M_1 müşterisi c doğrulamasını beklerken A düşmanının yaptığı çift harcama atağı.

Bitcoin ve diğer iş kanıtına dayalı para birimleri bu tarz atakları bir blok oluşturmak için hesaplama maliyetinin çok yüksek olmasıyla korur. Bu A düşmanının bir çift harcama yapması için hem çok fazla elektrik tüketimi yapması hem de gerekli donanıma sahip olması gerekmektedir. Bu şekilde yapılacak bir saldırı kazanılacak paradan çok daha maliyetli olacaktır.

PoW algoritmasındaki mekanizma nedeniyle tek başına blok üretme şansı düşük olan katılımcılar daha fazla blok üretebilme şansı elde edebilmek adına birlikte daha fazla

hesaplama gücüne sahip olabilecekleri madencilik havuzlarına katılmak isteyebilirler. 51 % hesaplama gücü elde edildiğinde, bu blockchaini kontrol altına alabilirler. Bu durum 51% saldırısı olarak da tanımlanmaktadır (Courtois ve Bahack, 2014; Eyal ve Sirer, 2013). 51% saldırısı için PoW algoritmasında madencilik havuzunun en az 51%'lik dilimine sahip olmak gerekirken PoS algoritması göz önüne alındığında bütün kripto paraların en az 51%'ine sahip olunması gerekmektedir.

2.5. Blockchain Türleri

Mevcut blockchain sistemleri farklı ihtiyaçlara göre açık, özel veya konsorsiyum tiplerinde kurgulanabilir. Açık blockchainde bütün kayıtlar herkese açıktır ve herkes konsensüs sürecinde yer alabilir. Örneğin kişilerin birbirine para gönderip almalarını sağlayan blockchain sistemleri kişilerin anonim olduğu fakat işlemlerin açık bir şekilde izlenebildiği bir açık blockchain yapısına sahiptir. Konsorsiyum blockchainde sadece önceden seçilmiş düğümler konsensüs sürecinde yer alabilir. Diğer bir ifade ile konsorsiyum blockchainde birkaç kuruluş tarafından oluşturulan gruplardaki düğümlerin sadece küçük bir kısmı konsensüs belirlemek için seçilir. Özel blockchainde ise yalnızca belirli bir kuruluştan gelen düğümlerin uzlaşma sürecine katılmasına izin verilir. Üç farklı blockchain türünün karşılaştırması Tablo 2.2'de görülebilir (Zheng, Xie, Dai, Chen ve Wang, 2017).

Tablo 2.2. Açık blockchain, özel blockchain ve konsorsiyum blockchain türlerinin karşılaştırması

Özellik	Açık Blockchain	Konsorsiyum Blockchain	Özel Blockchain
Ortak Karar Verme	Bütün Madenciler	Seçilen bilgisayarlar	Tek Organizasyon
Okuma İzni	Herkes	Herkes ya da kısıtlı kullanıcı	Herkes ya da kısıtlı kullanıcı
Veri Değiştirme İhtimali	Neredeyse imkansız	Değiştirilebilir	Değiştirilebilir
Verimlilik	Düşük	Yüksek	Yüksek
Merkezilik	Hayır	Kısmen	Evet
Konsensüs Süreci	İzinsiz	İzne tabi	İzne tabi

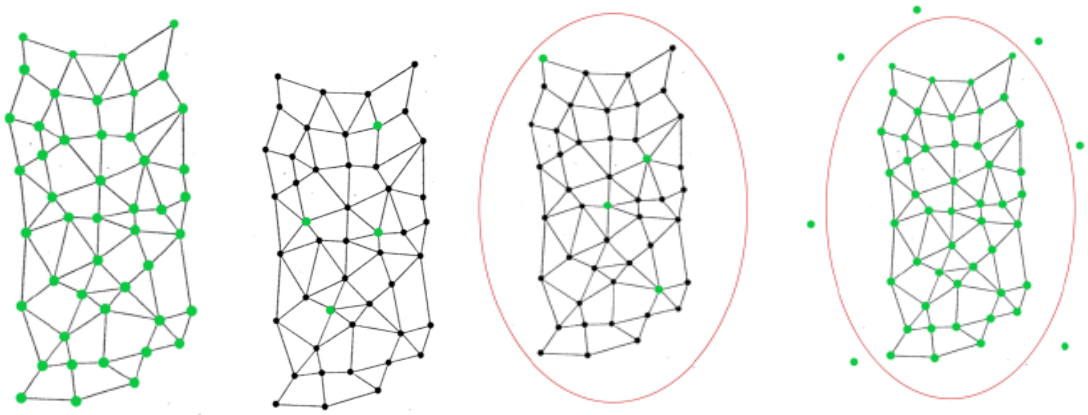
Açık blockchainde merkezi bir otorite yoktur ve blockchain isteyen herkesin erişimine açıktır. Ağdaki bir varlık okuma, işlem gönderme ve doğrulama hakkına sahiptir. Açık blockchain sistemlerinde sistem güvenliği binlerce farklı kullanıcı tarafından sağlandığı için sisteme kaydedilen bilginin geriye dönük olarak değiştirilmesi imkansıza yakındır.

Bu açıdan bakıldığı zaman en güvenli ve şeffaf blockchain türüdür. Ağda kötü niyetli düğümler ağın yarısından fazlasına (%51 saldırısı) sahip olmadığı müddetçe ortaya bir problem çıkmaz. Açık blockchain sistemlerde ağda çok fazla düğüm olmasından kaynaklı olarak doğrulama süreci uzun sürdüğünden verimlilik düşüktür.

Konsorsiyum blockchain sistemlerinde sadece seçilen makineler sisteme katılarak karar verme sürecinde söz sahibi olabilir. Blockchain verisi herkese açık olabileceği gibi erişilebilirliğin kısıtlandığı karma blok yapılar oluşturulabilir. Sistemde kısmi bir merkeziyetçi yapı hakimdir. Kullanıcı sayısı açık blockchaine göre daha az olduğundan verimlilik yüksektir. Açık blockchain kadar güvenli ve şeffaf bir sistem değildir.

Özel blockchain sistemlerinde blockchaine yazma yetkisi sadece özel bir gruba aittir. Blockchain verisini okuma hakkı herkese açık olabileceği gibi kısıtlamalar yapılabilir. Genellikle yüksek güvenlik gerektiren bilgileri yöneten kurumların blockchain teknolojisinden faydalanabilmeleri amacıyla kullanılır.

Ayrıca blockchain türlerini izne tabi (permissioned) ve izinsiz (permessionless) olarak iki farklı şekilde sınıflandırmak mümkündür (Usta ve Doğantekin, 2017). İzin gerektiren blockchainlerde sadece yetkili düğümlerin blok oluşmasına ve mutabakata katılmasına izin verilirken izin gerektirmeyen blockchainlerde ise tüm düğümler blok oluşturarak mutabakata katılabilir. Bu anlamda blockchain türleri izne tabi ve izinsiz olarak sınıflandırıldığında açık izinsiz (public permissionless), açık izne tabi (public permissioned), konsorsiyum (private permissioned) ve özel izinsiz (private permissionless) blockchain olarak sınıflandırılabilir (Meijer, 2017). Şekil 2.10.'da dört farklı blockchain tipinin görselleri yer almaktadır. Görseldeki yeşil düğümler konsensüs mekanizmasında yer alan doğrulayıcı düğümleri, siyah düğümler okuma/yazma düğümlerini ve kırmızı daire ise özel bir blockchain ağını temsil etmektedir.



Şekil 2.10. a) Açık İzinsiz b) Açık İzne Tabi c) Konsorsiyum (Özel İzne Tabi) d) Özel İzinsiz blockchain tipleri

Yapı bu haliyle tekrar değerlendirildiğinde açık izinsiz blockchain tipinde, blockchainden veri okuma ve göndermede ve konsensüs işleminde bir kısıtı olmayan blockchainin en temel halidir. Bitcoin ve Ethereum örnek verilebilir.

Açık izne tabi blockchain tipinde, blockchainden data okumada ya da işlem göndermede kısıt yoktur. Buna karşılık konsensüs işleminde yer almada kısıtlama vardır. Açık izne tabi blockchainin bir örneği Ripple'dır.

Konsorsiyum blockchain tipi özel izinsiz tipindeki blockchaine benzer olmasına rağmen en önemli fark, özel izinsiz yapıda sadece tek bir kuruluş içerisinde konsensüse varılmasıdır. Fakat konsorsiyum defterleri, mutabakat sürecinde birden fazla organizasyon içerir. Böyle bir defter türü, uçtan uca bir sürece dahil olan birden fazla varlığın olduğu yönetim veya tedarik zinciri için yararlı olabilir. Bu tür bir defter, bir işletme veya işletme modeli olarak daha fazla hizmet vermektedir (Meijer, 2017). Konsorsiyum blockchain, genellikle bankacılık sektöründe kullanılmaktadır. Konsensüs süreci önceden belirlenmiş düğümler tarafından gerçekleştirilir. Örneğin 15 finansal kuruluşun olduğu bir konsorsiyumda her kurumu bir düğüm temsil edebilir ve bir bloğun geçerli olabilmesi için 10 düğümün her bloğu imzalaması gerekebilir.

Özel izinsiz blockchain tipi genellikle tek bir organizasyon içerisinde tutulur. Özel blockchain, işlemleri içeriden doğrulayabilen grupları ve katılımcıları kurarak blockchain teknolojisinden faydalanmanın bir yoludur. Kendi bilgilerini kamuya açık olarak paylaşmak istemeyen kurumlara yönelik faydaları ortaya çıkarır. İşlem

doğrulama bir kuruluş içerisinde gerçekleştiği için, fikir birliği süreci çok daha hızlı gerçekleşir (Meijer, 2017).

2.6. Ethereum Akıllı Sözleşmeler

Akıllı sözleşme, bir işi yöneten sözleşme ve kuralları yerine getiren blockchain ağları üzerinde çalışan uygulamalardır. Farklı paydaşlar arasındaki dijital sözleşmelerin blockchain üzerinde tanımlanmasını sağlar. Merkezi bir otoriteye ihtiyaç duyulmadan taraflar arasında tanımlanan akıllı sözleşmeler, anlaşma şartlarının sağlanması durumunda hedeflenen aksiyonların otomatik olarak hayata geçirilmesini sağlar (Ünsal ve Kocaoğlu, 2018). Birden fazla sektörün farklı ihtiyaçlarına hizmet etme imkanı sunabilecek akıllı sözleşmeler blockchain teknolojisinin sunduğu en önemli özelliklerinden birisidir.

Bitcoin'in ortaya çıkmasından sonra, arka plandaki teknolojinin sadece eşler arası (P2P) para transferleri için değil, farklı amaçlar için kullanılabileceği düşünülerek çalışmalara başlanmıştır. Akıllı sözleşmeler blockchain bağlamında incelenirse,

- İçinde bir şartın gerçekleşmesi durumunda gerçekleşecek işi (if-this-then-that) tanımlayan mantıksal akışların önceden yazılmış olduğu
- Merkezi olmayan dağıtık bir platform üzerinde saklanan
- Bağlı olduğu bilgisayar ağı tarafından çalıştırılabilen
- Güvenilirliği bir bilgisayar ağı tarafından doğrulanan
- Üzerinde bulunduğu yapı/platform üzerinde güncellemelere yol açabilen

ufak programlardır şeklinde tanımlanabilir (Usta ve Doğantekin, 2017).

Akıllı sözleşmeler, ilişkili tarafların kapsam üzerinde anlaşmalarından sonra hazırlanıp, kriptografik olarak imzalanmasından sonra blockchain ağına yüklenirler. Blockchain ağındaki sözleşmeler ağdaki diğer bileşenlerle etkileşim kurabilirler. Sözleşmede önceden belirlenmiş durumlar oluştuğunda otomatik olarak içerisinde tanımlanmış olan anlaşma koşullarının çalıştırılması sağlanır (Usta ve Doğantekin, 2017).

Ethereum akıllı sözleşmeleri C, Phyton, Fortran, Javascript gibi turing complete programlama dilleri kullanarak işlem emirlerin yazılmasına izin verir. Her ne kadar farklı programlama dilleri ile geliştirme yapılmasına izin verilse de Solidity dili

ethereum akıllı sözleşme geliştirenlerin ilk tercihidir. Solidity, ethereum ekibi tarafından geliştirilen nesne tabanlı açık kaynak kodlu bir programlama dilidir. Akıllı sözleşme için yazılan programlar tüm ethereum düğümlerinde bulunan Ethereum Sanal Makinesi (EVM) tarafından çalıştırılır. EVM, ethereum akıllı sözleşmelerinin çalışabilmesi için bir çalıştırma ortamıdır. Bir EVM içinde çalıştırılan her bir işlem aynı anda eş zamanlı olarak ağdaki her düğüm tarafından da çalıştırılır. Her düğüm, istenilen şartların sağlanıp sağlanmadığını kontrol eder. Akıllı sözleme kodunu çalıştırmak için ethereum sisteminin para birimi olan Ether ile ödeme gerçekleştirilir. Ödenecek Ether miktarı, gerekecek hesaplama gücüne bağlı olarak değişir.

2.7. Ethereum Hesapları

Ethereum'da kullanıcı hesabı (EOA) ve sözleşme hesabı olarak iki farklı hesap tipi vardır. Kullanıcı hesaplarını kullanabilmek için bir özel anahtara ihtiyaç duyulur, işlem gönderilebilir ve bir kod ile ilişkilendirilmemişlerdir. Sözleşme hesapları ise ethereum blockchainde belirli bir adreste varlığını sürdürür ve kod değeri taşır. Ethereum blockchain, kullanıcı hesaplarından yapılan işlemlerle harekete geçirilir. Kullanıcı hesabının başlattığı bir işlem hedefi, bir başka kullanıcı hesabı veya bir sözleşme adresi olabilir. Kullanıcı hesaplarından sözleşme hesabına yapılan işlemlerde akıllı sözleşmenin kodu otomatik olarak çalıştırılır. Sözleşme hesapları bir kullanıcı hesabından tetiklenebileceği gibi başka bir sözleşme tarafından da tetiklenebilir. Sözleşme kodu, yeni blokların doğrulanmasının bir parçası olan ağdaki her düğümde EVM tarafından çalıştırılır ("Account Types, Gas, and Transactions", 2019).

2.8. Ethereum Ağları

Bir açık ağ ve özel ağ farklı odaklara sahip olmasına rağmen temelde aynı teknolojidir. Açık blockchain bütün işlemlerin şeffaflığını benimserken özel blockchain bilginin kötüye kullanılmasını önlemek için işlemlerin gizliliğine önem verir.

Ethereum ana ağı, ethereum blockchainin canlı ortamıdır. Gerçek verilerle işlemler yapılır ve işlemler için "gas" ödenir. Canlı ortamdaki bir hata hem finansal açıdan tehlikeli olabilir hem de ethereum blockchaindeki değişikliklerin kalıcı ve değiştirilemez olmasından kaynaklı kötüye kullanım durumları oluşturabilir. Canlı ortamda bu gibi problemlerle karşılaşmamak için ethereum test ağları kullanılabilir.

Ethereum ana ağı ve test ağları arasındaki tek fark farklı ağlarda yönetiliyor olmalarıdır. Ethereum geliştirmeciler için üç farklı test ağı sunmaktadır. Bu test ağları Ropsten, Kovan ve Rinkeby'dir. Ropsten, iş kanıtı (PoW) konsensüs algoritması kullanırken Kovan ve Rinkeby, otorite ispatı (PoA) algoritması kullanmaktadır.

Bir ethereum özel ağı, ana ethereum ağından bağımsız olan tamamıyla özel bir ağdır. Kurumların ethereum özel ağını kullanmalarındaki ana sebep saklanan özel verilerin ilgili organizasyon dışından erişilebilirliğini engellemektir. Sadece doğru yetkilere sahip olan düğümler blockchain ağındaki konsensüs sürecine katılabilir. Bu özel ağdaki düğümler ana ethereum düğümlerine bağlanamaz ve erişimleri sadece bu özel blockchain ile sınırlandırılır. Ethereum özel ağları, test yapmak veya blockchaini deneyimlemek amacıyla da açık ağlar yerine kullanılabilir. Özel ethereum ağları dağıtık veri tabanı gibi davranır, özel bir ağ olduğundan özel verileri içerebilir, erişim izini gerektirir. Özel blockchain yapısının açık blockchain yapısına göre avantajları aşağıdaki şekilde sıralanabilir.

- İşlemler ucuz veya ücretsizdir.
- İşlemler daha hızlı gerçekleştirilir.
- Blockchain üzerinde daha fazla yetkiye ve kontrole sahip olunur.

2.9. Blockchain ile Merkezi ve Dağıtık Veri tabanları Karşılaştırması

Blockchain, birbirine bağlı bloklarda salt okunur bir veri yapısındadır. Bir blok içerisindeki verilerin düzenlenmesine veya silinmesine izin veren hiçbir merkezi izin yoktur.

Dağıtık veri tabanı, aynı ağda veya tamamen farklı ağlarda farklı noktalarda bulunan iki veya daha fazla sunucudan oluşan bir veri tabanıdır. Dağıtık veri tabanının merkezi veri tabanlarına göre farklı avantajları vardır. Bir sunucuda güç kesintisi veya bir donanımsal problem meydana gelmesi durumunda sunucuların farklı lokasyonlarda olması sistemin devamlılığı açısından önemlidir. Ayrıca yük paylaşımı yapılarak daha çok kullanıcıya daha kısa sürede yanıt vermesi de sağlanır. Fakat merkezi ve dağıtık veri tabanlarında, veriler kolayca değiştirilebilir veya silinebilir. Genellikle, verilerin herhangi bir bölümünde ve/veya yapısında değişiklik yapabilen veri tabanı yöneticileri vardır. Ancak blockchain yapısında verilerin değiştirilmesi veya silinmesi mümkün değildir.

Blockchain ile merkezi ve dağıtık veri tabanlarından kilit farklılıkları Tablo 2.3.'de gösterilmiştir (Bozic ve diğerleri, 2016). Blockchain kayıtların bütünlüğü, erişilebilirlik, hata toleransı ve güvenilir düğüm işbirliği ile diğer sistemlere göre üstünlük sağlar. Blockchain tabanlı sistemler genel olarak gizlilik hedeflememektedir.

Tablo 2.3. Blockchain ile merkezi ve dağıtık veri tabanları karşılaştırması

Özellikler	Blockchain	Merkezi Veritabanı	Dağıtık Veritabanı
Kayıtların Doğruluğu	Yüksek	Orta	Orta
Erişilebilirlik	Yüksek	Düşük	Orta
Hata Toleransı	Yüksek	Düşük	Yüksek
Gizlilik	Düşük	Yüksek	Orta
İşlem Zamanı	Düşük	Yüksek	Orta
Güvenilir Düğüm İşbirliği	Yüksek	Düşük	Düşük

2.10. Blockchain Teknolojisinin Kullanım Alanları

Blockchain teknolojisinin sahip olduğu özelliklerin keşfedilmesiyle beraber birbirinden farklı sektörler bu teknolojiden faydalanabilmek adına çalışmalarını, planlamalarını ve duyurularını yapmaya başlamıştır.

Sağlık sektörü, geleneksel sistemlere dayanan ve değişim ihtiyacı duyan bir sektördür. Hastalara ait verilerin güvenli depolanması ve paylaşılması gibi önemli konular hastanelerin karşılaştığı zorluklardan birisidir. Güvenlik gerektiren verilerin güvenli bir şekilde saklanması ve yetkilere göre paylaşılması, blockchain teknolojisinin kullanılabileceği bir alandır. Tedarik zinciri yönetiminde merkezi bir otoriteye ihtiyaç duyulmadan taraflar arasında gerekli şartların sağlanması durumunda ödemeler otomatik hale getirilebilir. Blockchain teknolojisinin sağladığı geriye dönük işlemlerin değiştirilememesi veya silinememesi ve süreçlerin taraflar arasında şeffaflıkla izlenebilmesi ticaret yönetimi için önem teşkil etmektedir. Finans alanında para transferleri, dijital kimlik yönetimi, doküman yönetimi gibi uygulamalarda kullanılmaktadır (Kırbaş, 2018).

Hükümetlerin önemli bir görevi bireyler, varlıklar, faaliyetler ve organizasyonlarla ilgili güvenilir bilgiler sağlamasıdır. Örneğin devlet eliyle yürütülen kimlik bilgileri, mülkiyet kayıtları, ceza faaliyetleri, oy verme gibi kritik önem taşıyan verilerin yönetimi karmaşık ve zor olabilir. Blockchain teknolojisinin sağladığı şeffaflık ve

güven veri yönetimini kolaylaştırma imkanı sunabilir. Kamu sektörü kuruluşları, ihtiyaçları doğrultusunda farklı blockchain tiplerini kullanarak uygulamalarını bu teknolojiye entegre edebilir. Özel alanlardaki blockchain uygulamalarından elde edilen prototip sonuçları, devlet işlerinde bu teknolojinin faydalarını kullanmaya teşvik etmektedir. Gelişimi ve değişimi devam eden bu yeni teknoloji, devlet işleri için pilot uygulamalarla derin bir anlam kazanılması amacıyla araştırılmaya ve alınan başarılı sonuçlar sonrasında entegre edilmeye devam edilmektedir.

Güvenlik ve denetim için merkezi bir yapıdan ziyade dağıtık bir yapı oluşturulmasını gerektiren maliyetin yüksek olduğu durumlarda blockchain teknolojisi avantajlı hale gelmektedir. Küresel çapta blockchain teknolojisinin imkanlarından faydalanmak için ülkeler hem kendi içerisinde hem de kendi aralarında farklı anlaşmalar yapmaktadır. Örneğin Avrupa'da 22 ülkenin bir araya gelerek oluşturduğu Avrupa Blockchain Ortaklığı (EBP), üye ülkelerin bu teknolojiyi kullanarak geliştirdikleri teknolojilerin ve düzenlemelerin bir birlik sağlanarak yürütülmesini hedeflemektedir. Bu anlamda yürütülen çalışmaların parça parça uygulanması yerine geliştirilen blockchain uygulamalarının Avrupa Birliği ülkelerinde yaygınlaşması amaçlanmaktadır (Digibyte, 2018).

BÖLÜM 3. KRİPTOLOJİ TEMELLERİ

Blockchain teknolojisi özetleme, dijital imzalama, açık-özel anahtarlar gibi kriptografik yapı taşlarını kullanır. Bu bölümde kriptolojinin temellerinden bahsedilmiştir ve diğer bölümlerle ilgili kavramlara değinir.

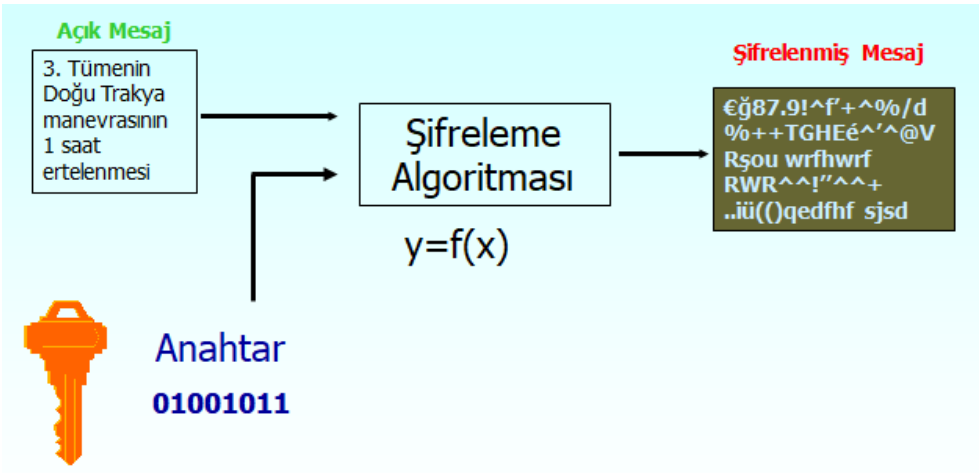
Kryptos (gizli dünya) ve logos (bilimi) kelimelerinden oluşan kriptoloji, kriptografi ve kriptanaliz olarak ikiye ayrılır. Kriptografi, iki veya daha fazla tarafın güvenli bilgi alışverişi yapmasını sağlarken bilginin istenmeyen taraflarca anlaşılmayacak bir hale dönüştürülmesinde kullanılan, temeli zor matematiksel problemlere dayanan teknikler ve uygulamaların bütünüdür. Kriptanaliz, kriptografinin tam karşıtı olarak kriptografik sistemlerin kurduğu mekanizmaları inceler ve şifrelenmiş verileri çözmeye çalışır (Kırımlı ve Erdem, t.y.). Kriptografi gizlilik, bütünlük, gönderici kimliğinin doğrulanması, inkâr edememe gibi Şekil 3.1.'de gösterilen bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemleri içermektedir (Akleylek ve diğerleri, 2011).

Şekil 3.1. Bilgi güvenliği unsurları

Temel bilgi güvenliği unsurları (Akleylek ve diğerleri, 2011):

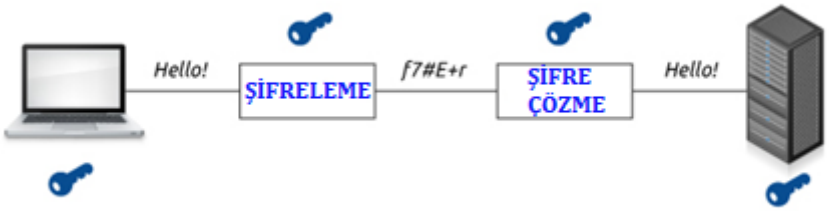
- Gizlilik: Bilgi istenmeyen taraflarca anlaşılmamalıdır.
- Bütünlük: Bilgi iletimi sırasında değişiklik yapılmadığı doğrulanmalıdır.
- Kimlik Denetimi: Gönderici ve alıcı birbirlerinin kimliklerini doğrulamalıdır.
- İnkar Edememe: Gönderici gönderdiği bilgiyi ve alıcı aldığı bilgiyi inkar edememelidir.

Bir gönderici tarafından bir alıcıya açık ağlar üzerinden bir ileti gönderilmek istenildiğinde, açık ağ üzerinden gönderilen bu ileti üçüncü kişiler tarafından dinlenebilir veya mesaj içeriği değiştirilebilir. Burada bahsi geçen ileti düz bir metindir. Düz metin, plaintext olarak da ifade edilebilir. Bir iletinin içeriğini üçüncü kişilerden saklamak amacıyla yapılan işlem şifrelemedir (encryption). Şifreleme işleminde bir anahtar ve şifreleme algoritması kullanılarak düz bir metin Şekil 3.2.'deki gibi şifreli bir metine dönüştürülmüş ve başkalarının anlayamayacağı hale getirilmiştir. Bu bilgi, bir yere iletilmek için şifrelenen bir mesaj veya şifrelenerek saklanan bir bilgi olabilir. Şifrelenen bir ileti şifreli metin (ciphertext), şifrelenmiş metni düz metne çevirme işlemi ise şifre çözümüdür (decrypt) (Herranz, 2007).



Şekil 3.2. Bir metnin şifrelenmesi

Şifreleme ve şifre çözme işlemleri Şekil 3.3.'de gösterilmiştir.

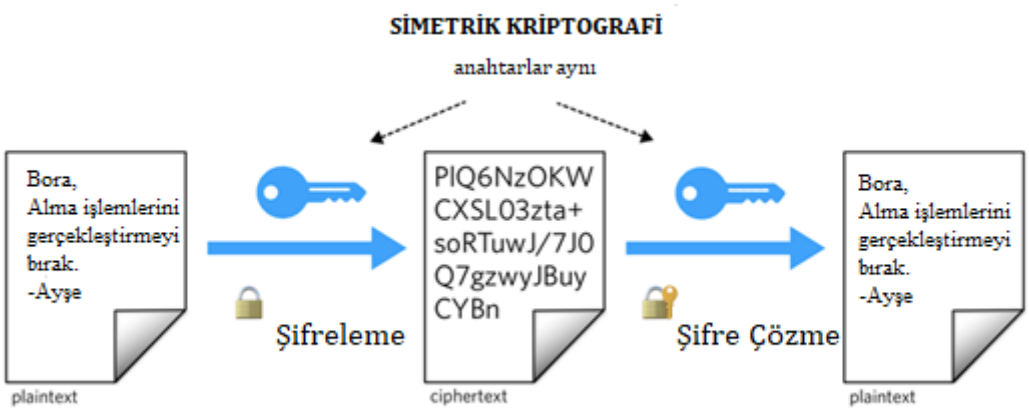


Şekil 3.3. Şifreleme-şifre çözme

Kriptografide şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre simetrik kriptografi ve asimetrik kriptografi olmak üzere iki tip kriptografik teknik vardır.

3.1. Simetrik Kriptografi

1976 yılına kadar mevcut şifre sistemlerinin güvenilirlikleri gizli anahtara dayanmaktaydı. Hem bilgi gönderen tarafın şifrelemede hem de bilgiyi alan tarafın şifre çözmede aynı anahtarı kullanmasına dayanan yapı, gizli anahtarlı sistemler olarak adlandırılır. Bu yöntemi kullanarak gizli veri alışverişi yapacak taraflar arasında simetrik anahtar emniyetli bir şekilde paylaşılmalıdır (Nath, Ghosh ve Alam Mallick, 2010; Thakur ve Kumar, 2011). Simetrik kriptografinin gösterimi Şekil 3.4.'de yer almaktadır.

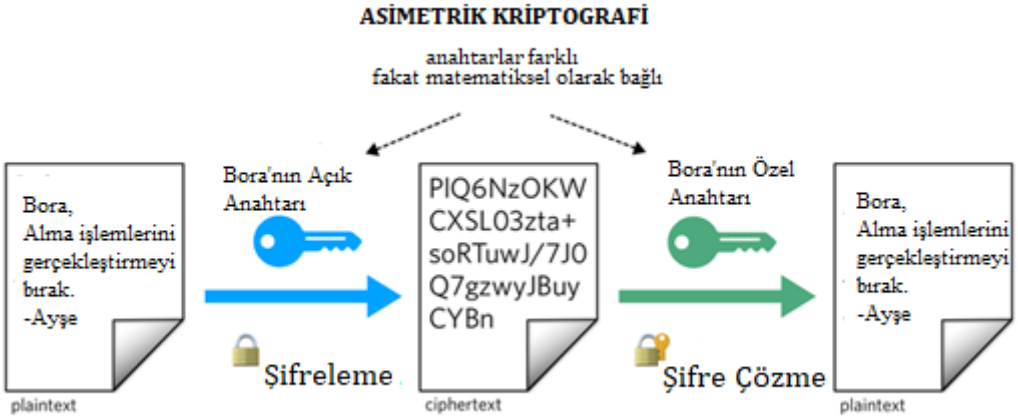


Şekil 3.4. Simetrik kriptoloji

3.2. Açık Anahtar – Asimetrik Kriptografi

Açık anahtar sistemlerinin keşfedilmesiyle aynı anahtarın hem gönderici hem de alıcı tarafından bilinmeden de güvenli haberleşme yapılabileceğini ortaya çıkartmıştır (Akleylek ve diğerleri, 2011). En yaygın açık anahtarlı kriptografi kullanımı şifreleme ve sayısal imzalamadır. Açık anahtar kriptografi, bir diğer adıyla asimetrik kriptografi birbirinden farklı fakat birbiriyle ilişkili açık ve gizli olmak üzere iki anahtarlardan oluşan kriptografik yöntemdir. Bu yöntemde özel anahtarın açık anahtarla bir matematiksel bağlantısı vardır. Açık anahtar herkese dağıtılabilir fakat özel anahtar sadece sahibinde muhafaza edilmelidir. Açık anahtar, plaintexti şifrelemede ve özel anahtar ise şifre çözmede kullanılır. Açık anahtar kullanılarak bir şifreli mesaj gönderildiğinde sadece mesajın sahibine ait olan açık anahtarın eşi özel anahtar kullanarak şifreli mesaj açılabilir.

Bu kriptografi yönteminde her kullanıcının kendine ait bir açık bir de özel anahtar olmak üzere bir anahtar çifti vardır. Asimetrik kriptografi yapısı Şekil 3.5.'de gösterilmiştir.

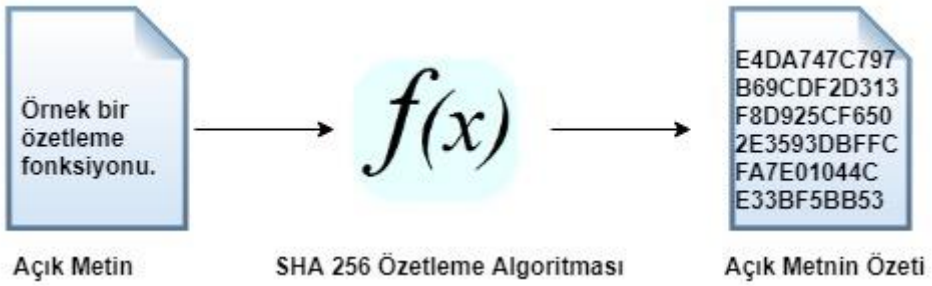


Şekil 3.5. Asimetrik kriptoloji

Açık anahtar kriptolojisi blockchain teknolojisinde de faydalanılan geniş kullanım alanı olan bir yöntemdir. Bu yöntem blockchain teknolojisinde işlemlerin gizli anahtar ile imzalanması, hesap adreslerinin açık anahtar olarak kullanımı, gizli anahtar ile imzalanmış işlemlerin açık anahtarla doğrulanması gibi işlemlerde kullanılmaktadır (Murat, 2018).

3.3. Kriptografik Özet (Hash) Fonksiyonları

Kriptografik özetleme fonksiyonları farklı uzunluklardaki girdilerden sabit uzunlukta çıktı üretirler. Bir hash fonksiyonu ile aynı girdiden aynı çıktı üretilirken farklı girdilerle aynı uzunlukta fakat farklı bir çıktı değeri üretilir. Girdideki bir harfin bile değişmesi çıktıyı tamamen değiştirebilir. Özetleme fonksiyonları geri dönüşümü olmayan tek yönlü fonksiyonlardır (Aslan, 2012). Özetleme fonksiyonunun çalışma biçimi Şekil 3.6.'da gösterilmiştir.



Şekil 3.6. Örnek bir özetleme fonksiyonu

Elektronik imza, metnin özeti alınarak gerçekleştirilir. Metin özeti alındıktan sonra metni imzalayan kişinin özel anahtarı ve asimetrik şifreleme kullanılarak mesaj özeti şifrelenir. Açık metinde değiştirilecek çok küçük bir değişiklik mesaj özetini de değiştireceği için imzalama işlemini geçersiz kılacaktır. Şifrelenen mesaj özeti açık metne eklenerek karşı tarafa gönderilir. Mesaj özetinden bir metne ulaşmak mümkün değildir.

Blockchain teknolojisinde kriptografik fonksiyonlardan yoğun bir şekilde yararlanılır. Bunlardan bir tanesi olan özetleme fonksiyonları, blockchain teknolojisinde de aktif olarak kullanılmaktadır. Özet fonksiyonlarının blockchainde en temel kullanımı her bloğun bir önceki bloğun özet bilgisini tutmasıdır (Murat, 2018).

BÖLÜM 4. AÇIK ANAHTAR ALTYAPISI (AAA-PKI)

AAA, bir güvenlik altyapısını sağlamak için birlikte kullanılan yöntemler ve teknolojilerle beraber şifrelemeyi güvenli bir şekilde kullanmak için dijital sertifikaların oluşturulması, yönetilmesi, dağıtılması, kullanılması ve iptal edilmesi için gereken ilkeleri ve prosedürleri tanımlar (Yu ve Ryan, 2017).

1970'li yıllara kadar sadece resmi ve askeri kurumlar tarafından kullanılan kriptografik yöntemler Whitfield Diffie ve Martin Hellman'ın 1976 yılında önerdiği Açık Anahtarlı Sistemler kavramıyla yeni bir boyut kazanmıştır. Bu tarihe kadar var olan şifreleme sistemlerinin güvenlikleri anahtarın gizliliğine dayanmaktaydı. Gizli anahtarlı sistemler olarak ifade edilen bu sistemlerde, şifreleme ve şifre çözme işlemi için taraflar arasında önceden belirlenen anahtarlar kullanılmaktaydı. Ancak açık anahtarlı sistemlerin keşfiyle beraber ortak gizli anahtarın bilinmeden de güvenli bir haberleşme sağlanabileceği ortaya çıkmıştır. Ayrıca açık anahtarlı sistemler, gizlilik, veri bütünlüğü, kimlik kanıtlama, inkar edememe konularına da çözüm getirerek yeni uygulamaları beraberinde getirmiştir. Açık anahtarlı sistemlerde herkes tarafından bilinen açık ve kişiye özel gizli anahtar ile gizli bir şekilde haberleşme sağlanmaktadır. Açık anahtar, şifreleme ve elektronik imza doğrulamada, gizli anahtar ise şifre çözme ve elektronik imza oluşturmada kullanılır. Birbirinden farklı olan iki anahtarın kullanıldığı açık anahtarlı sistemlerde güvenilirliğin sağlanması adına problemin çözümü zor olan matematiksel problemler kullanılmaktadır (Akleylek ve diğerleri, 2011). Bu algoritmalara çarpanlara ayırmanın zorluğuna dayanan RSA, sonlu cisimler ve eliptik eğri üzerindeki ayrık logaritma probleminin zorluğuna bağlı ECDSA (Elliptic Curve Digital Signature Algorithm), Elgamal, McEliece örnek verilebilir. Günümüzde en çok kullanılan ve bilinen çift anahtar şifreleme algoritması algoritma RSA olmasına rağmen bu algoritma hantaldır. Günümüzde Eliptik Eğri düşük anahtar boyutlarında güvenli şifreleme yaptığı için daha çok tercih edilmektedir. Bununla beraber SSL, SSH, TLS

gibi internet standartlarının altında asimetrik anahtar şifrelemesi kullanılmaktadır (Taş ve Kiani, 2018).

Açık anahtar sistemlerinde en yaygın kullanılan uygulamalardan bir tanesi de elektronik imzadır. Elektronik imzalar oluşturulurken RSA, ECDSA gibi kullanılacak algoritmanın belirlenmesinden sonra hangi donanımlar ile kullanılacağı önemlidir. En çok bilinen ve kullanılan elektronik donanımlardan birisi akıllı kartlardır. Akıllı kartlar ile imzalama, şifreleme, imza doğrulama, şifreleme çözme ve anahtar depolama gibi özellikler sunulmaktadır. Akıllı kartların kullanılabilmesi için kart okuyucular kullanılır (Akleylek ve diğerleri, 2011).

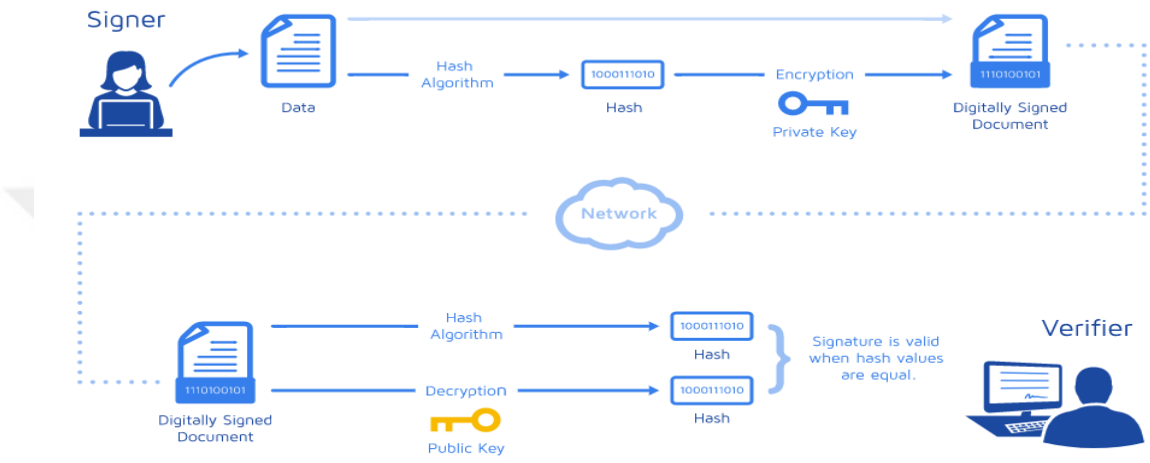
4.1. Elektronik İmzalar

İnternet üzerinde yapılan işlemlerde güvenlik en çok ihtiyaç duyulan unsurların başında gelmektedir. Günümüzde birbirinden farklı birçok alanda kullanılan elektronik imza kurumlar ve bireyler için farklı avantajlar sağlamaktadır. Elektronik ortamdaki bir metnin onaylanması, anlaşma veya sözleşmenin kabul edilmesi gibi ihtiyaçlar karşısında işlemlerin kolaylaşmasına imkan verilmesi için kanunlarda yer alan sözleşmelerin şekli ve ispatlarına ilişkin hükümlerin yeniden düzenlenmesine ihtiyaç duyulmuştur. Ülkemizde elektronik imza kullanımı 5070 sayılı Elektronik İmza Kanununun yürürlüğe girmesiyle beraber 2004 yılında başlamıştır (Resmi Gazete, 2004). Bu anlamda elektronik imzaların elektronik ortamda gerçekleşen işlemlerde ıslak imza gibi hukuksal bağlayıcılığı bulunmaktadır. Elektronik imza kullanım oranları günden güne artmaya devam etmektedir. Hızlı artışın başlıca sebepleri arasında elektronik imza fiyatlarının düşmesi, iş süreçlerinin elektronik imzayı gerektirecek şekilde yenilenmesi gibi nedenler olduğu söylenebilir.

Şifreleme yöntemleri sayesinde elektronik imzalı bir belgenin sahibinin tespiti için imza sahibinin kimliği imzalanan veriyle ilişkilendirilir. Elektronik imza, Şekil 4.1.'de gösterildiği gibi mesaj içeriği ile mesajı imzalayan kişiye ait asimetrik özel anahtarın birlikte kullanılması ile elde edilir.

Sayısal (Dijital) imza ve elektronik imza kavramları günlük hayatta ve birçok akademik çalışmada aynı anlamda kullanılmalarına rağmen birbirinden farklıdır. Sayısal imza belirli yöntemlerle sayısallaştırılmış imzayı ifade etmek için kullanılırken, elektronik

imza ıslak imza yerine elektronik ortamda üretilen bütün teknolojileri kapsayan bir üst kavramı ifade eder. Sayısal imza, bir verinin asimetrik yöntemle şifrelenmesi ve şifrenin çözülmesi temeline dayanan kriptografik bir yazılım teknolojisidir. Elektronik imza, sayısal imzayı da kapsayan bir üst kavram olarak başka elektronik imza çeşitlerini de içerir (Yılmaz, 2016). Bu nedenle açık anahtarlı kriptografide kullanılan sayısal imza aynı zamanda bir elektronik imza uygulamasıdır.



Şekil 4.1. Elektronik imza

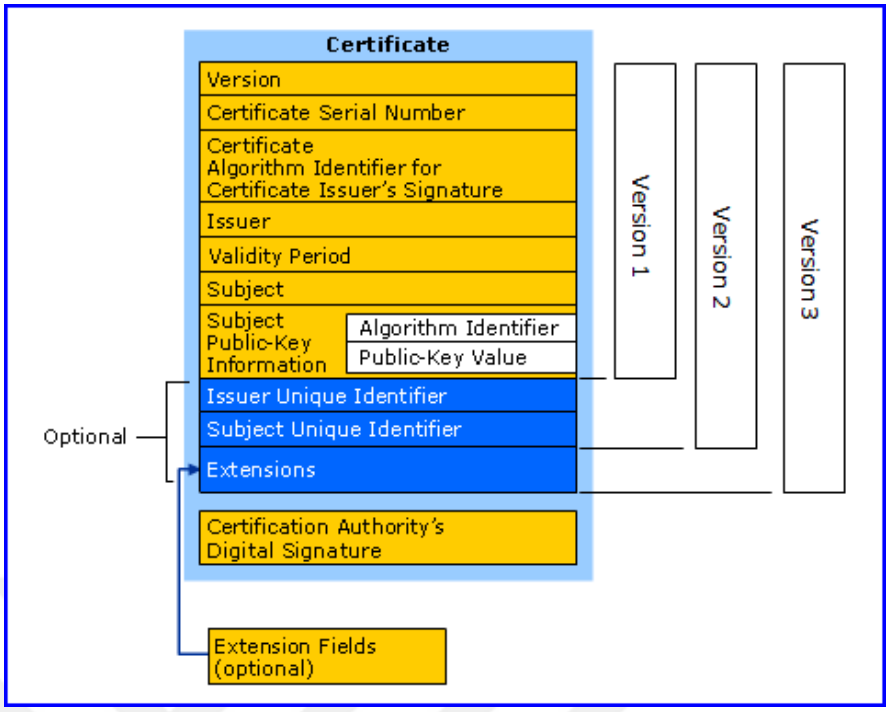
Elektronik imza uygulamasında kullanılan asimetrik şifreleme yöntemine göre birbiriyle haberleşmek isteyen tarafların kendilerine ait bir gizli ve bir açık anahtarı vardır. Gönderilecek mesaj bir özetleme algoritmasıyla özgün bir şekilde özeti alınarak özgün bir şekilde kısaltılır. Buna özet (hash) alma denir. Göndericinin özel anahtarı kullanılarak mesajın özeti ile elde edilen yeni değeri kodlanır. Gönderilen mesaj herhangi bir şekilde değişirse özet değeri ilk halinden farklı olacaktır. Yani elektronik imza, mesaj ve özel anahtara özgüdür. Elektronik imza, mesajın sonuna eklenerek alıcıya iletilir. Alıcı, imzalı mesajı gönderen kişinin açık anahtarını kullanarak çözer. Çözülen bu değer ve mesajın özet değeri aynı ise gönderilen ve alınan metnin aynı olduğu durumda mesajda bir değişiklik yapılmadığı ya da herhangi farklı bir hatanın meydana gelmediği tespit edilmiş olur (Yalçınkaya, 2008). Ayrıca elektronik imza göndericinin özel anahtarıyla imzalandığı için mesajın gönderici tarafından gönderilmediği iddia edilemez.

5070 sayılı Elektronik İmza Yasası'na uygun güvenli elektronik imza, nitelikli elektronik sertifika (NES) kullanılarak oluşturulur (Resmi Gazete, 2004). NES, X.509 standardına uygun olarak üretilir ve bu standartla uyumlu olan akıllı kartlara yüklenebilir.

4.2. Elektronik Sertifikalar

Elektronik sertifikalar, kişinin kimliğini elektronik ortamda ispatlaması için kimlik kartı, sürücü belgesi veya diğer kimlik belgelerinde kullanılan elektronik dosyalardır. Elektronik sertifikalar sertifika makamları tarafından düzenlenir (Erzincan, 2004). Elektronik sertifikalar açık anahtar kriptografi yöntemini kullanır ve kamuya açıktır. Elektronik sertifikalar kurumlara, kişilere veya web sunucularına ait olabilir ve ait olduğu varlıkların bilgilerinin elektronik ortamda güvenli bir şekilde iletilmesini sağlar.

X.509, AAA sistemlerinde en yaygın kullanılan sertifika standartlarının başında gelir. IETF (The Internet Engineering Task Force) tarafından RFC 5280'de detayları belirtilen ve dünyaca kabul gören sertifika standardıdır (Boeyen ve diğerleri, 2008). Şekil 4.2.'deki gibi bu sertifikaya yeni eklemeler yapılarak v1, v2, v3 olarak üç farklı sertifika sürümü ortaya çıkmıştır. X.509 v3, diğer iki türde bulunan tüm özellikleri kapsayan en son sertifika sürümüdür. RFC 5280'de İnternet X.509 PKI sertifika yapısı için tüm temel alanlar, farklı işlevleri karşılayan eklentiler ve bunların yapıları ayrıntılarıyla anlatılmıştır.



Şekil 4.2. X.509 sertifika alanları (Shafa'amry ve Alam Aldeen, 2009)

X.509 v3 sertifikalar için temel alanlar şu şekilde özetlenebilir (Hasircioğlu ve Öz, 2008):

- Sürüm: X.509 standardının v1, v2, v3 olarak tanımlanan sürümünü belirtir.
- Sertifika Seri Numarası: SM tarafından tekil olarak her sertifikaya verilen ve SM ismi ile birlikte sertifikayı tanımlayan bu alan pozitif bir değerdir. Yayınlayan adı (issuer name) ve sertifika seri numarası tek bir sertifikaya özeldir.
- İmzalama Algoritması: Sertifikayı imzalamak için SM tarafından kullanılan algoritma tanımlayıcısını içerir. Bu bilgi açık anahtar alanında yer alan algoritma bilgisi ile aynı olmalıdır (Ör. sha256RSA).
- Sertifikayı Yayınlayan: Sertifikayı imzalayan ve yayınlayan kuruluş bilgisini içerir.
- Geçerlilik Periyodu: Sertifika başlangıcı ve sonu olarak sertifikanın geçerli olduğu tarihleri belirtir.
- Konu: SM'nin sertifikayı verdiği bilgisayar, kullanıcı, ağ aygıtı veya hizmetin adını belirtir.
- Açık Anahtar: Sertifika ile ilişkilendirilmiş anahtar çiftinin açık anahtarını içerir.
- SM İmzası – Parmak İzi: SM tarafından imzalanan dijital sertifikanın içeriğinin özetidir.

Sürüm 1 ve 2 alanlarına ek olarak, X.509 sürüm 3 sertifikaları, sertifikaya ek işlevler ve özellikler sağlayan uzantılar içerir. Bu uzantılar isteğe bağlı olarak sertifikayı yayınlayan SM tarafından sertifikaya eklenebilir. En çok kullanılan X.509 v3 uzantıları aşağıdaki şekildedir:

- Hizmet Sağlayıcı (Yetkili) Anahtarı Tanımlayıcısı – Özne Anahtarı Tanımlayıcısı: Bir üst SM sertifikasındaki Özne Anahtarı Tanımlayıcı alanı ile sertifikadaki Hizmet Sağlayıcı Anahtarı Tanımlayıcı alanlarındaki değerler aynı olmalıdır.
- Sertifika İlkeleri: Bir kuruluşun bir sertifika vermeden önce bir sertifika isteğinin kimliğini doğrulamak için hangi önlemleri aldığını açıklar.
- Temel Kısıtlamalar: Sertifikanın kullanılacağı işlemler ile ilgili bir kullanım kısıtlaması olması durumunda söz konusu kısıtı tanımlayan ibarenin kendisi ve bu ibareye ait nesne belirteci bu alana yazılır.
- CRL Dağıtım Noktaları: Sertifikayla ilgili yayımlanacak SİL'e ulaşmak için gerekli bilgiyi içerir.
- Yetkili Bilgi Erişimi: ESHS bilgi ve servislerine ulaşmak için kullanılır. Farklı erişim bilgilerinin olması halinde bu bilgiler liste halinde bu eklentide yer alır.
- Anahtar Kullanımı: Veri imzalama, veri şifreleme vb. gibi sertifikanın kullanım amacını belirtir.

Sertifikanın imzası, sertifikayı imzalayan üst SM'nin açık anahtarı ile kontrol edilir. Fakat öncesinde sertifikayı imzalayan üst SM'nin sertifika geçerlilik kontrolü yapılır. Sertifika zincirindeki tüm sertifikalar için imza doğrulama işlemi yapılması gerektiği için güvenilir olan kök sertifika ya da güvenilir olan başka bir sertifikaya kadar yol üzerindeki tüm sertifikaların doğrulama işlemi gerçekleştirilir. Bir sertifikanın üst sertifika bilgisine ulaşmak için sertifikadaki Hizmet Sağlayıcı Erişim Bilgisi kullanılabilir. Bu eklentide SM sertifikasının HTTP veya LDAP adresi bulunur. Erişim yöntemleriyle SM sertifikası doğrulamaya bu şekilde devam edilir.

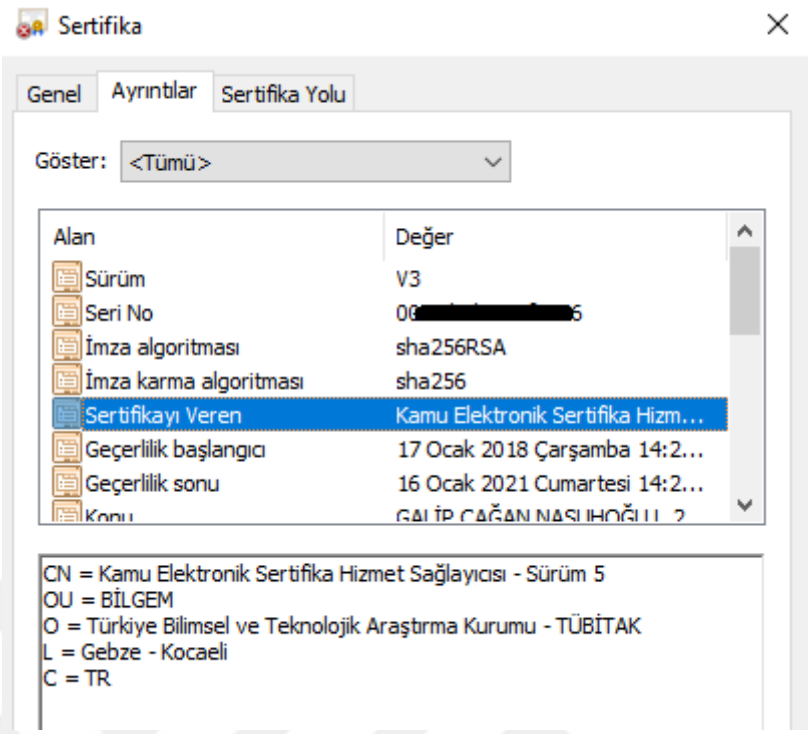
4.3. NES (Nitelikli Elektronik Sertifika)

Nitelikli Elektronik Sertifika (NES)'ya dayanarak oluşturulan elektronik imzaların elektronik ortamda gerçekleştirilen işlemlerde ıslak imza gibi hukuksal bağlayıcılığı bulunmaktadır. Hızla dijitalleşmenin devam ettiği günümüzde sağlık, finans, lojistik gibi birbirinden farklı sektörlerde hizmet veren firmalar faaliyetlerini dijital ortama taşımış veya taşımaktadır. Dijital verilere güvenin sağlanması açısından elektronik imza büyük önem teşkil etmektedir. T.C. Elektronik İmza Kanununun 9 uncu maddesinde detayları belirtilen NES özetle, ESHS (Elektronik Sertifika Hizmet Sağlayıcı)'nin kimlik bilgileri ve kurulduğu ülke adını içeren, imza sahibinin kimliğinin tespitinin sağlanabildiği, sertifika geçerlilik süresinin başlangıç ve bitiş tarihini, sertifika seri numarası gibi bilgileri barındıran elektronik sertifikalardır (Resmi Gazete, 2004). Sertifikalar X.509 standardına uygun olarak üretilir ve bu standart ile uyumlu web uygulamaları, akıllı kartlar ve akıllı çubuklara (token) yüklenebilir.

T.C.5070 sayılı Elektronik İmza Kanunu'na göre bir NES sertifikasında bulunması zorunlu alanlar aşağıdaki şekildedir (Resmi Gazete, 2004).

- Sertifikanın "Nitelikli Elektronik Sertifika" olduğunu belirten ibare.
- ESHS kimlik bilgileri ve kurulduğu ülke adı.
- İmza sahibinin tespit edilebileceği kimlik bilgileri.
- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi.
- Sertifikanın geçerlilik zamanını gösteren başlangıç ve bitiş tarihleri.
- Sertifika seri numarası.
- Sertifika sahibi bir başkası adına hareket ediyorsa bu yetkiye ilişkin bilgi.
- Sertifika sahibinin talebi doğrultusunda mesleki veya diğer kişisel bilgiler.
- Varsa sertifika kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ait bilgiler.
- ESHS'nin sertifikada yer alan bilgilerini doğrulayan güvenli elektronik imzası.

Şekil 4.3.'de bir NES'e ait görsel bulunmaktadır.

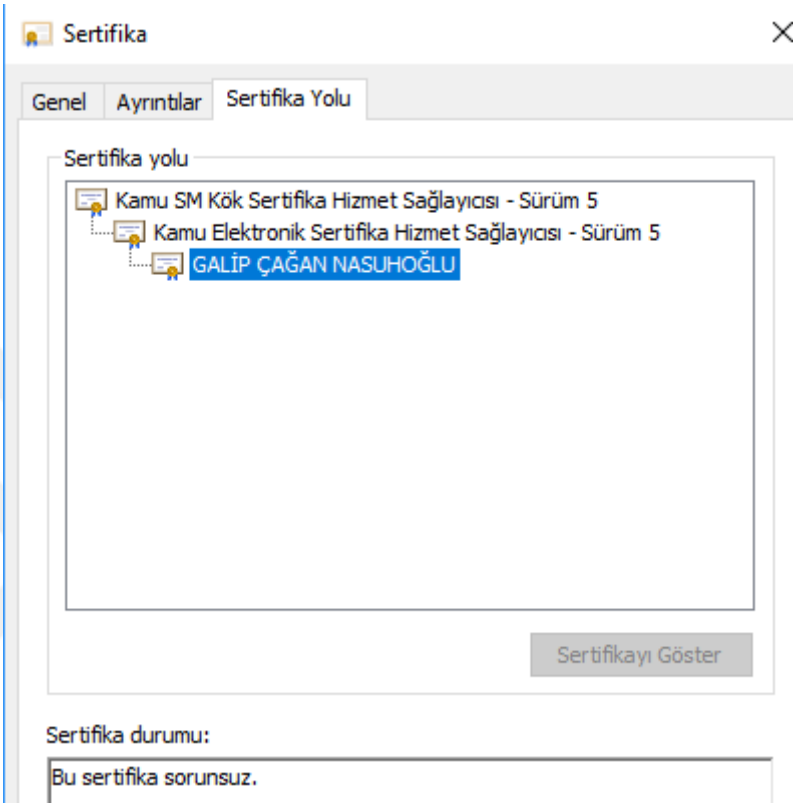


Şekil 4.3. Örnek bir NES'de yer alan ayrıntılar.

4.4. Elektronik Sertifika Hizmet Sağlayıcılar (ESHS) – Sertifika Makamları (SM)

AAA sistemlerinde her varlığa SM'ler tarafından ilgili varlığın kimliğiyle ilişkilendirilmiş sertifikalar dağıtılmaktadır. Bu anlamda bir açık anahtarın kime ait olduğunu gösteren bir belge niteliğindedir. Bir elektronik sertifika ile yapılan her işlemde sertifikanın geçerlilik kontrolünün yapılması önemlidir. Çünkü bir sertifika herhangi bir nedenle her an geçerliliğini yitirebilir ve geçerliliğini yitiren bir sertifika ile işlem yapılması geri dönüşü olmayan sorunlara neden olabilir. Bütün elektronik sertifikalar yetkili bir SM tarafından yayınlanır ve her SM'nin de kendi sertifikası vardır. SM'ler kendi aralarında kök sertifika makamı ve alt kök sertifika makamı olarak ayrılır. Bir SM doğrudan güven kaynağı kabul edilerek kendi kendisinin sertifikasını imzalıyor ise kök sertifika makamı, güvenilir bir üst SM tarafından imzalanarak yayınlanmış ise alt kök sertifika makamı olarak tanımlanır. Bir sertifikanın güvenilir bir sertifika olduğundan emin olmak için o sertifikayı yayınlayan SM'nin imzasına bakılır. Bu nedenle geçerlilik süreci için sadece işlem yapılan sertifika değil, aşağıdaki şekilde de görülebileceği gibi sertifikayı yayınlayan ESHS sertifikalarının geçerlilikleri de

kontrol edilerek sertifika yolu üzerindeki tüm sertifikaların bu şartları sağlaması gerekmektedir (Başçi, 2008). Şekil 4.4.'de bir NES'te yer alan sertifika yolu gösterilmiştir.



Şekil 4.4. Sertifika yolu

Güvenilir olarak kabul edilen SM'lerin ürettiği sertifikaların içerdiği bilgilerin mutlak doğru varsayılması güvenlik problemlerine neden olabilmektedir.

5070 sayılı Elektronik İmza Kanununu gereği Türkiye'de elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenleme ve ESHS'lerin faaliyetlerini denetleme görevi Telekomünikasyon Kurumu'na (TK) verilmiştir. TK, kanunda belirtildiği şekilde gerekli gördüğü zamanlarda ESHS'leri denetleme hakkına sahiptir (Resmi Gazete, 2005). İlgili Başbakanlık genelgesi ile kamu kurum ve kuruluşları için 2005 yılında TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü bünyesinde bir sertifikasyon merkezi olan Kamu Sertifikasyon Merkezi (Kamu SM) kurulmuştur (Yılmaz, 2016). Türkiye'nin ilk ESHS'si olan Kamu SM,

5070 Elektronik İmza Kanunu'na uygun olarak kurulmuş olup günümüzde çalışmalarına devam etmektedir. Kamu kapsamının dışındaki sertifika başvuru sahiplerine yönelik olarak, Kanundaki ilgili şartları sağlayarak TK denetiminden geçen yetkili ESHS'ler elektronik sertifika hizmetleri verme hakkına sahip olabilirler.

ESHS'ler varlıklara elektronik sertifikalar vermenin yanı sıra sertifika iptal bilgilerini yayınlama, zaman damgası, dizin hizmeti de sağlarlar.

4.5. Sertifika Geçerlilik Kontrol Süreci

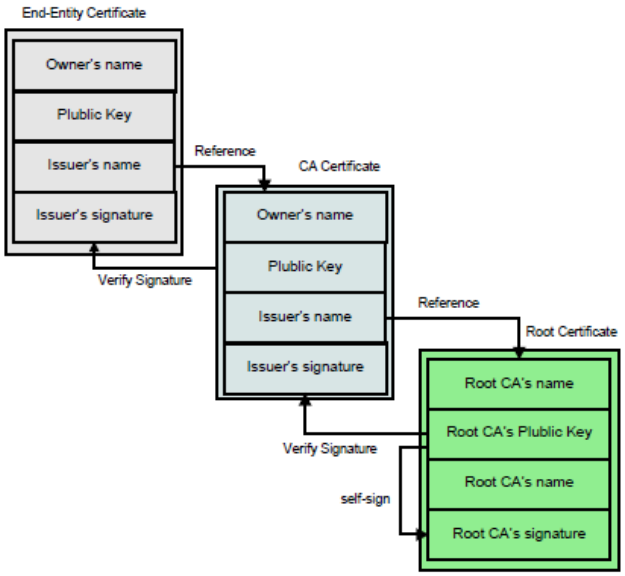
Elektronik imza açısından elektronik sertifikalar kişinin kendisini elektronik ortamda ispatlaması için kullanılan elektronik dosyalar olarak tanımlanabilir. Diğer bir ifade ile AAA anahtar çifti ile nüfus cüzdanı, ehliyet gibi inkar edilemez bir kimlik bilgisini kriptografik olarak birbirine bağlayan elektronik kayıtlardır. Elektronik sertifika ile atılan bir imzanın geçerli kabul edilebilmesi için belirli kriterlere göre geçerli olması ve iptal edilmediğinin teyit edilmesi gerekir. Bir sertifikanın geçerliliği anlık ya da geçmiş bir zaman için kontrol edilebilir (Başçi, 2008).

Bir elektronik sertifika ile yapılan her işlemde sertifikanın geçerlilik kontrolünün yapılması önemlidir. Çünkü bir sertifika herhangi bir nedenle her an geçerliliğini yitirebilir ve geçerliliğini yitiren bir sertifika ile işlem yapılması geri dönüşü olmayan sorunlara neden olabilir. Bütün elektronik sertifikalar yetkili bir SM tarafından yayınlanır ve her SM'nin de kendi sertifikası vardır. SM'ler kendi aralarında kök sertifika makamı ve alt kök sertifika makamı olarak ayrılır. Bir SM doğrudan güven kaynağı kabul edilerek kendi kendisinin sertifikasını imzalıyor ise kök sertifika makamı, güvenilir bir üst SM tarafından imzalanarak yayınlanmış ise alt kök sertifika makamı olarak tanımlanır. Kullanıcı sertifikaları ise alt kök SM'ler tarafından imzalanarak yayınlanan, sertifika imzalama özelliği olmayan sertifikalardır ve elektronik imzalamada kişinin kendisini ispatlaması için kullanılırlar. Bir kullanıcı sertifikası ile kök sertifikası arasındaki bağlantı sertifika zinciri olarak tanımlanır. Buradaki önemli nokta, kullanıcı sertifikası ile kök sertifikası arasında bir ya da birden fazla alt sertifika makamı sertifikası olabilir (Yakubov ve diğerleri, 2018). Bu nedenle geçerlilik süreci için sadece işlem yapılan sertifika değil, sertifikayı yayınlayan ESHS sertifikalarının geçerlilikleri de kontrol edilerek sertifika yolu üzerindeki tüm sertifikaların bu şartları

sağlaması gerekmektedir. Bir sertifikanın geçerli kabul edilebilmesi için aşağıdaki kriterleri sağlaması gerekmektedir. RFC 5280 standardına göre bir sertifikanın geçerli sayılabilmesi için bu sertifikadan güvenilir kabul edilen sertifikaya kadar yol üzerindeki tüm sertifikaların bu şartları sağlaması gerekmektedir (Boeyen ve diğerleri, 2008).

- Sertifikanın güvenilir köklerden üretilmiş olması gerekmektedir. Eğer sertifikayı yayınlayan ESHS kök değil ise alt kök olan ESHS'lerin sertifikalarının bulunması ve bu alt köklerin de sertifikalarının geçerlilikleri ve imza geçerlilikleri kontrol edilmelidir.
- Sertifika geçerlilik süresini ifade eden başlangıç ve bitiş tarihlerinin doğrulama zamanını kapsaması gerekmektedir.
- Geçerliliği kontrol edilen hiçbir sertifikanın iptal edilmemiş olması gerekmektedir.

Şekil 4.5. son varlıktan güven zincirinin başladığı kök-SM'ye kadar olan güven zincirini ifade eder.



Şekil 4.5. Sertifika güven zinciri (Yakubov ve diğerleri, 2018)

Bir sertifikanın üst kökünü bulmak için sertifikanın içerisindeki bilgilerden faydalanılır. Sertifikaların içerisinde yer alan Özne/Konu Anahtar Tanımlayıcısı (SKI) sertifikanın kendisini ve Yetkili Anahtar Tanımlayıcısı (AKI) ise sertifikayı üreten kök sertifikanın özne anahtar tanımlayıcısını gösterir. Bir sertifikanın üst kökünü bulmak için içerisinde

bulunan yetkili anahtar tanımlayıcısı bilgisi ile tüm kök sertifikaların özne anahtar tanımlayıcıları karşılaştırılır. İki değer birbirine eşit olduğunda da sertifikanın kökü bulunmuş olur. Fakat sadece sertifikayı bulmak yeterli değildir. Bulunan sertifikanın da geçerliliğinin ve imzasının kontrol edilmesi gerekmektedir. Sertifikanın iptal durumu ise; sertifikayı üreten ESHS'nin yayınladığı SİL'e bakarak, ya da ESHS'ye ait OCSP sunucu aracılıyla olmak üzere iki şekilde öğrenilebilir (Başçi, 2008). SİL yönteminde sertifika durum bilgilerine ait iki güncelleme arasında bir bekleme zamanının bulunması sertifikaların durumunun tam anlamıyla garanti edilememesine sebep olur. Bir sertifikanın iptal kontrolü yapılmak istendiğinde SİL içerisindeki listeden ilgili sertifikanın seri numarası aranır. İlgili sertifikanın seri numarası SİL'de bulunursa bu sertifika iptal edilmiş, bulunamazsa bu sertifika SİL'e göre geçerli kabul edilir. Bu da yüksek güvenlik gerektiren durumlar için güvenlik açığı yaratan bir durumdur. Bununla beraber iptal kontrolü yapılacak her bir sertifika için SİL dosyalarının yeniden indirilip kontrol yapılması kurumlara büyük yükler getirmektedir. SİL yerine çevrimiçi bir yöntem kullanılması ile sertifikanın sorgulanan andaki cevabı alınarak hatalı işlem olasılığı azaltılmış olur. Bu nedenle bir internet bağlantısı varsa çevrimiçi yöntemler tercih edilmelidir. Fakat çevrimiçi OCSP yöntemi de hem tek nokta hatası hem de sertifikanın geçmiş günlüklerine erişim konusunda yetersiz kalmaktadır.

BÖLÜM 5. AAA SERTİFİKA İPTAL UYGULAMALARI

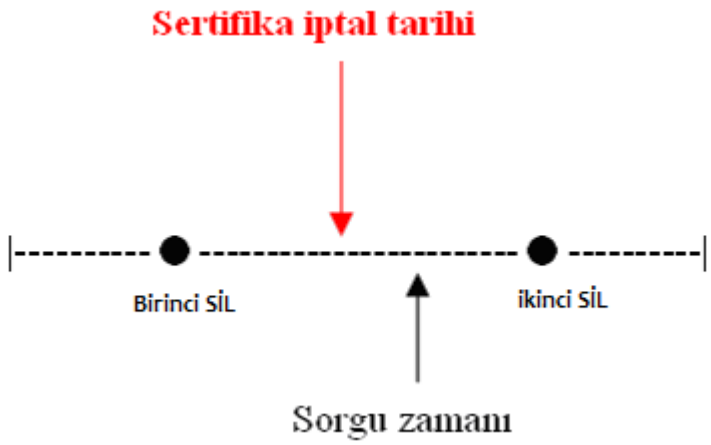
Elektronik sertifikaların birçok nedenden dolayı durum bilgisi değişebilir. Sertifikanın özel anahtarı kaybedilmesi, sertifika sahibinin bilgileri değiştirilmesi gibi farklı sebeplerle sertifikanın iptal edilmesi gerekebilir. Ayrıca belli bir süre kullanılmayacak olan sertifikanın askıya alınması, askıdaki sertifikanın tekrar geçerli duruma getirilmesi sertifika iptali dışındaki sertifika durum değişikliklerine örnek verilebilir. AAA, sertifika durumu güncellenmesi için gerekli altyapıyı sağlamaktadır. Geleneksel AAA yapısı SM tabanlıdır ve sertifikaların iptal bilgileri ilgili SM tarafından yayınlanır. Sertifika iptal durumlarının sorgulanması için farklı yöntemler bulunmaktadır. Sertifika durum yönetimi çevrimiçi veya çevrimdışı olarak yapılabilir. Sertifikaların iptal bilgisi için en yaygın kullanım, SM'lerin belirli aralıklarla SİL dosyaları yayınladığı çevrimdışı yöntem ile anlık OCSP cevaplarının aldığı çevrimiçi yöntemdir (Başçi, 2008). Çevrimdışı yöntemler kullanıldığında, sertifika durum bilgilerine ait iki güncelleme arasında uzun bir zaman aralığı bulunduğundan sertifikaların durumu tam anlamıyla garanti edilemez. Fakat bu durum bazı uygulamalar için yeterlidir. Çevrimiçi yöntemler ise, çevrimdışı yöntemlerle elde edilenden daha güncel sertifika durum bilgisine ihtiyaç duyulduğunda kullanılır. Genellikle, yüksek güvenlik gerektiren durumlarda çevrimiçi yöntemlerin kullanılması tercih edilir (Öğretmen, t.y.). Bazı durumlarda hem çevrimiçi hem de çevrimdışı yöntemler bir arada kullanılabilir.

5.1. Sertifika İptal Listesi (SİL/CRL)

Sertifika iptal listeleri, X.509 tipindeki sertifikalarla birlikte ilk olarak 1988'de ITU-T tarafından ortaya atılmıştır. 1993 yılında ise ikinci sürümüne erişmiştir (International Telecommunication Union, 1997).

SİL'ler, Yetkili ESHS'ler tarafından çevrimdışı olarak belirli periyotlarla yayınlanan elektronik imzalı bir dosyadır. SİL dosyasında iptal edilmiş sertifikaların seri numaralarını, iptal tarihlerini, kendi oluşturulma ve bir sonraki güncelleme tarihlerini

içeren bilgiler yer alır. İsteğe bağlı olarak sertifikaların iptal neden bilgilerini de içerebilir. SİL, yayınlayıcısı tarafından sayısal olarak imzalanır ve böylece SİL geçerliliği de kontrol edilebilir. Bir sertifika için iptal kontrolü yapılacağı zaman öncelikle söz konusu sertifikayı yayınlayan SM'nin yayınladığı SİL'in imzası kontrol edilir, eğer imza doğruysa ilgili sertifikanın seri numarası SİL'de aranır. Eğer seri numarası listede bulunuyorsa sertifika iptal edilmiş demektir, listede yoksa sertifika SİL'e göre geçerli kabul edilir. Çevrimdışı yöntemler kullanıldığında, sertifika durum bilgilerine ait iki güncelleme arasında Şekil 5.1.'deki gibi uzun bir zaman aralığı bulunduğundan, sertifikaların güncel durumu tam anlamıyla garanti edilemez (Öğretmen, t.y.). Şekil 5.1.'de, birinci SİL'in yayınlanmasından 2.ci SİL'in yayınlanmasına kadar olan süre içinde bir sertifika iptal edilmiştir. Birinci SİL yayınlandıktan sonra yeniden bir sorgulama yapılmış fakat bu arada henüz yeni SİL yayınlanmadığı için sertifika geçerli sayılmıştır. Bu da yüksek güvenlik gerektiren durumlar için güvenlik açığı yaratan bir durumdur (Başçi, 2008).



Şekil 5.1. Bir sertifika iptal durumu

Yüksek güvenlik gerektiren durumlarda çevrimiçi bir yöntemin kullanılmış olması sertifikanın güncel durumdaki bilgisine ulaşılmasını sağlar ve hatalar önlenmiş olur. Bu nedenle bir internet bağlantısı varsa çevrimiçi yöntemler tercih edilmelidir.

AAA yönetiminin en kritik adımlarından birisi sertifikaların iptalinin denetlenmesidir. Bir sertifika, normalde belirtilen bitiş tarihinden önce iptal edilebilir. Bu şekilde iptal edilen bir sertifikanın geçerliliği de iptal edilmesiyle beraber sona erer. Bir sertifika

farklı sebeplerle geçersiz duruma gelebilir. RFC 5280, X.509 sertifika standardı ayrıca sertifika iptal uygulamalarını da kapsayan bir standarttır. Standarda göre sertifika iptal nedenleri ve kodları aşağıdaki gibidir (Boeyen ve diğerleri, 2008):

- 0→Belirsiz / Unspecified
- 1→Anahtar çalınma / Key Compromise
- 2→SM anahtar çalınma / CA Key Compromise
- 3→Bilgi değişimi / Affiliation Changed
- 4→Yerini almak geçersiz hale getirmek / Superseded
- 5→Sertifika Otoritesi'nin faaliyetini sona erdirmesi / Cessation of Operation
- 6→Askıya alma / certificateHold
- 7→ - (kullanılmamakta)
- 8→İptal listesinden çıkarma / removeFromCRL
- 9→Hak mahrumiyeti / privilegeWithdrawn
- 10→Üst Sertifika Otoritesi'nin anahtarının çalınması / aACompromise

5.2. OCSP (Çevrimiçi Sertifika Durum Protokolü)

OCSP, RFC 6960'ın içindeki Internet Engineering Task Force (IETF)' da tanımlanmış bir PKI teknolojisi standardıdır (Başçi, 2008). OCSP yönteminde, sertifikaya ait sertifika geçerlilik bilgisi çevrimiçi olarak SM'nin sağladığı sunucudan alınabilir. İstek – cevap mantığı ile çalışır. X.509 sertifikaları için tasarlanmış olmasına rağmen farklı tipteki sertifikalarla da çalışabilir. İptal edilen sertifikalar anında OCSP sunucusuna bildirilir. İstemciler, OCSP sunucularına birer istekte bulunur ve durumunu öğrenmek istedikleri sertifikayı göndererek sunucu tarafından imzalanmış bir cevap alırlar. Gelen bu cevap içerisinde de sertifikanın durumu bulunmaktadır. OCSP, SİL'in gecikme, ölçeklenebilme ve yönetim sorunlarına çözüm getirmek için SİL'e tamamlayıcı olarak geliştirilmiştir (Başçi, 2008). OCSP yöntemi, SİL yönteminin yerine kullanılabilir. Bazı durumlarda ise bu iki yöntem beraber kullanılabilir. Böylece sorgulanan sertifikaya ait en güncel durum bilgisi elde edilebilir.

OCSP sunucusundan istemcinin talep ettiği sertifika için "Anlamlı" sertifika durum bilgisi cevabı aşağıdakilerden biri olabilir (Santesson ve diğerleri, 2013):

- İyi / good
- İptal edilmiş / revoked
- Bilinmeyen / unknown

"İyi" durumu, sertifika geçerlilik sorgulamasında alınan olumlu bir yanıttır. En azından bu yanıt sertifikanın OCSP yöntemine göre iptal edilmediğini gösterir. Fakat "iyi" durumu, sertifikanın yayınlandığı veya alınan cevabın ilgili sertifikanın geçerlilik süresi içinde üretildiği anlamına gelmez. "İptal edilmiş" durumu, sertifikanın kalıcı bir şekilde iptal edilmiş veya askıya alınmış olduğunu belirtir. "Bilinmeyen" durumu ise, OCSP sunucusunun durumu sorgulanan sertifika hakkında bilgiye sahip olmadığını gösterir. OCSP yanıtı, OCSP sunucusu tarafından sayısal olarak imzalanır. Herhangi bir hata durumunda OCSP yanıtı bir hata mesajı içerir (Öğretmen, t.y.).

Çevrimiçi bir sertifika durum sorgulama protokolü olan OCSP'nin internet gibi dışarıya açık bir sistem üzerinde çalışması beraberinde bazı güvenlik problemlerini getirmektedir. Bu bakımdan OCSP cevap saldırılarına karşı savunmasızdır. Örneğin "İyi" durumu barındıran imzalı bir OCSP yanıtı, istemci ile sunucu arasında bir düşman tarafından yakalanarak saklanabilir. Geçerliliği sorgulanan sertifikanın herhangi bir sebepten iptal edilmesinden sonra istemci söz konusu sertifikayı tekrar sorguladığında düşman tarafından istemciye daha önceden saklanmış olan "iyi" yanıtının döndürülmesi bu duruma örnek olarak verilebilir. OCSP, nonce kullanarak bu güvenlik açığının üstesinden gelebilir. Buna karşılık, birçok OCSP yanıtlayıcısı ve birçok müşteri nonce değerinin kullanımını desteklemez (Öğretmen, t.y.). Bir başka güvenlik açığı, bir müşterinin bir OCSP yanıtlayıcısından makul bir süre içinde yanıt almaması durumunda protokol ihmal edilir ve güvenliği ihlal edilmiş olan sertifikayı kabul eder.

SİL ve OCSP arasında büyük bir hız farkı da vardır. SİL'in ortalama büyüklüğü 1MB civarındadır (üretilmiş olan 100000 sertifika için ortalama değer), OCSP'lerin ise 4KBdır. Aradaki bu fark ciddi bir hız farkına yol açar (Başçi, 2008).

BÖLÜM 6. AAA TABANLI ELEKTRONİK SERTİFİKA DURUM BİLGİSİ YÖNETİMİNDE TEMEL SORUNLAR VE ÇÖZÜM ÖNERİLERİ

SM tabanlı AAA sistemlerin önemli sorunlarından birisi sertifika durum bilgilerinin güvenilirliğiyle ilgilidir. Güvenilir bir sertifika iptal bilgisi için çevrimiçi bir yöntem kullanılmalı ve merkeziyetçi bir yapıdan uzak olmalıdır. Mevcut yapıdaki diğer bir ihtiyaç ise son kullanıcının bir sertifika için güvenilir bir yapıda sadece mevcut durum değil aynı zamanda geçmişe dönük sorgulama yapabilmesini sağlamaktır.

Blockchain temel olarak değer içeren para, kimlik gibi verilerin dijital ortamda açık ve güvenli bir şekilde depolanması ve yönetilmesi için tasarlanmış bir teknoloji olarak tanımlanabilir (Yıldırım, 2015). Bütün işlemlerin kaydını tutan veri tabanı dağıtık defter olarak tanımlanır ve defterden bir bilgi silme imkanı yoktur. Blockchain, çoğunlukla Bitcoin ve Ethereum gibi kripto paraların başarısına tanık olduktan sonra birbirinden farklı sektörlerde en ilgi çeken teknolojilerin başında gelmeye başlamıştır. Özellikle yüksek güvenilirlik gerektiren, veri hata ve hilelere kapalı olması gereken sistemler blockchain teknolojisine ilgi duymaktadır (Yakubov ve diğerleri, 2018).

İçinde iş mantığı taşıyan blockchain teknolojisi tabanlı akıllı sözleşmeler, birbirinden farklı sektörlerde devrim yaratacak dijital özellikleri desteklemekte ve bunu ise blockchain teknolojisinin sunduğu zaman damgalı ve sonradan değiştirilemez güvenilir bir veri bütünlüğü sağlayarak gerçekleştirmektedir (Yıldırım, 2015). Blockchain teknolojisi sahip olduğu özellikler sayesinde AAA sistemlerinin temel problemlerinden olan tek nokta hatasının giderilmesini ve güvenilir işlem kayıtlarının tutulmasını sağlar. Blockchain işlemlerinin ağ üzerinde sürekli olması ve ayrıca zaman damgalı ve düzenli olması önemli bir avantajdır. AAA sistemlerin bir hizmeti olan sertifika iptal bilgileri için blockchain teknolojisi kullanılarak güncel, merkeziyetçi yapıdan uzak ve kullanıcı odaklı bir yapı oluşturulabilir. Bu tür bir özellik, özellikle sertifika iptal verileri için

önemlidir, çünkü tutarsız veya güncel olmayan bilgiler geçersiz bir sertifikanın kullanılmasına yol açabilir. Ek olarak blockchain tabanlı AAA, açık ve sadece yazılabilen işlem günlükleri özelliğiyle doğal olarak Google tarafından önerilen Sertifika Şeffaflığı (Certificate Transparency) özelliğine de benzemektedir.

6.1. Sertifika İptal Sistemlerinde Geçmiş Günlüklerin Tutulmaması

AAA sistemlerinin sorunlarından bir tanesi kullanıcıların sertifikaların geçmiş günlüklerine erişiminde yaşadığı kısıtlamadır. Bir sertifikanın iptal edilmesi ile sertifikanın geçerliliği, normalde belirtilen bitiş tarihinden önce sona erer. Bu şekilde son kullanım zamanından önce iptal olan bir sertifika gerçek iptal tarihi gelene kadar her SİL'de yayınlanır. Sertifika bitiş tarihi geçtikten sonra ise genellikle dosya boyutlarını arttırmaması için SİL'de yayınlanmaz. Bu şekilde iptal edilen bir sertifikanın sertifika sağlayıcıları tarafından ne zaman iptal edildiğinin bilgisine günümüz SM tabanlı AAA teknolojisiyle erişmek geriye dönük sorgulamalar yapılarak külfetli bir işlem gerektirir. Bunun yanında sertifika iptal listeleri askıya alınan sertifikaları da içerebilir. Bir sertifika, bir süre için askıya alındığında sertifika iptal edilmiş gibi işlem görür. SİL içerisindeki listede askıya alınan bir sertifika, işlem tipi iptal olan sertifikalardan farklı bir değer alarak ayırt edilebilir. Fakat çevrimiçi yöntemi olan OCSP, istek-cevap mantığıyla çalıştığından sertifika için anlık olarak iyi, iptal edilmiş veya bilinmeyen bilgileri alınabilir (Santesson ve diğerleri, 2013). Örneğin geçmişte bir süre için sertifikası askıya alınan bir kullanıcının sertifikası bu sürede içerisinde kötü amaçlarla kullanılabilir. Böyle bir durumda hangi tarihlerde sertifikanın askıya alındığının bilgisine erişilmesi ihtiyacında hem SİL hem de OCSP yöntemleri yetersiz kalmaktadır. Mevcut yapıda, SM tarafından yayınlanan SİL dosyaları yedekleniyorsa bu dosyalar tek tek kontrol edilerek geçmişe dönük aramalarla bilgiye ulaşılmaya çalışılır, yetersiz kalındığı durumlarda ise SM yetkilisinden destek istenir. Diğer taraftan OCSP yönteminde ise sadece sertifikanın güncel durumunu gösteren anlık sorgulamalar yapılabilmektedir. OCSP yönteminde geriye dönük sorgulama yapılamadığından bu sorgulama yöntemi de yetersiz kalmaktadır.

Bu çalışmada son kullanıcılar, sertifikaların güncel ve geriye dönük durum bilgilerine kolay bir şekilde erişerek sorgulama yapabilir. Bu sorgulama ayrıca adli işlemlerde de verimlilik sağlayabilir. Elektronik imza ile ilgili geçmişe dönük olarak elektronik

sertifika durumlarının tarihçesini gerektiren olası adli bir durum ile karşılaşılabilir. Böyle bir durumda ilgili kişi tarafından sürekli güncel, güvenilir ve kullanıcıya kolaylık sağlayan bir yapı üzerinden başka bir üçüncü kişiye ihtiyaç olmadan sorgulamalar gerçekleştirilebilir.

6.2. Çevrimdışı Yöntemlerin Yeterince Güvenilir Olmaması

Sertifika iptal durumlarının sorgulanmasında farklı metotlar ortaya atılmıştır. Sertifika durum yönetimi çevrimiçi veya çevrimdışı olarak yapılabilir. Bazen her iki metodun birlikte kullanıldığı durumlarla da karşılaşılabilir (Öğretmen, t.y.). Günümüzde en çok kullanılan çevrimdışı yöntemine SİL, çevrimiçi sertifika durum yönetimine ise OCSP metodu örnek verilebilir (Başçi, 2008). SİL yönteminde sertifikalara ait geçerlilik bilgisi SM tarafından önceden oluşturulur ve sistemde yer alan kullanıcıların erişebileceği ortak bir alana yerleştirilir. OCSP yönteminde ise, geçerlilik durumu sorgulanan sertifikaya ait durum bilgisi çevrimiçi olarak sertifika otoritesinin sağladığı servisler tarafından alınabilir. SİL yönteminde sertifika durum bilgilerine ait iki güncelleme arasında bir bekleme zamanının bulunması sertifikaların durumunun tam anlamıyla garanti edilememesine sebep olur (Öğretmen, t.y.). Bir sertifikanın iptal kontrolü yapılacağı zaman SİL içerisindeki listeden ilgili sertifikanın seri numarası aranır. İlgili sertifikanın seri numarası SİL'de bulunursa bu sertifika iptal edilmiştir, bulunamazsa bu sertifika SİL'e göre geçerli kabul edilir. Bu da yüksek güvenlik gerektiren durumlar için güvenlik açığı yaratan bir durumdur. Bununla beraber iptal kontrolü yapılacak her bir sertifika için SİL dosyalarının yenden indirilip kontrol yapılması kurumlara büyük yükler getirmektedir. Örneğin TCKK gibi kullanıcı sayılarının milyonları bulduğu sistemlerde SİL dosyası 120 MB'lere erişebilmektedir. Böyle büyük bir dosyanın indirilmesi zaman açısından çok yavaş olacak ve internet bant genişliğini tüketecektir (Başçi, 2008). Böyle bir sistem SİL dosyalarında sertifika sorgulanması veya sertifikanın geçmiş bir dönemde durumu ile ilgili bilginin elde edilmesi için kullanışlı değildir. Fakat çevrimdışı yöntemler bazı uygulamalar için yeterlidir. Çevrimiçi yöntemler ise, çevrimdışı yöntemlerle elde edilenden daha güncel sertifika durum bilgisine ihtiyaç duyulduğunda kullanılır. Sertifika iptal bilgilerinin sürekli olarak kullanılabilirliği ve güncel tutulması çevrimiçi hizmetler için çok

önemlidir. Genellikle, yüksek güvenlik gerektiren durumlarda çevrimiçi yöntemlerin kullanılması tercih edilir (Öğretmen, t.y.).

Bu çalışmada yüksek güvenlik gerektiren durumlar ve güncel sertifika iptal bilgilerine ihtiyaç duyulması göz önüne alınarak blockchain teknolojisi ile alternatif bir çevrimiçi yöntem anlatılmaktadır.

6.3. SM Tabanlı AAA Sistemlerinde Tek Nokta Hatası

Günümüz AAA sistemlerin temel hata noktalarından birisi olan tek nokta hatası (Single Point of Failure - SPoF) sertifika iptal bilgilerinin güvenilirliği ve güvenliği ile ilgilidir. Bu yapıya göre her SM sadece kendi imzaladığı sertifikaların iptal bilgisinden sorumludur. Sertifikaları ve SM'leri içeren uzun bir saldırı listesi mevcuttur (Chen ve diğerleri, 2018). Tüm bu saldırı olayları ve SM kesintileri, iptal edilen sertifikalar için güvenilir, zamanında ve yüksek oranda erişilebilir bilgiye duyulan ihtiyacı işaret etmektedir. Ayrıca farklı SM'lerin yayınladığı sertifikaların iptal kontrollerinin yapılmasını gerektiren bir durumda her SM'nin kendine özel SİL dosyalarına bakılması gerekmekte ve bu durum sertifika kontrolünde karışıklığa neden olabilmektedir.

Geleneksel AAA yapısındaki tek merkeziyetçi sorununu çözmek için bu çalışmada birden çok SM'nin merkezi olmayan ve güvenilir bir ortak defteri paylaşarak sertifika iptal bilgilerini tuttuğu yöntem öneriliyor. Çalışmada, elektronik sertifikaların durum güncellemesi sadece sertifikayı yayınlayan kaynak SM tarafından işaretlenerek blockchain platformunda tutulur. Blockchain teknolojisinin merkezi olmayan yapısı sayesinde SM'ye erişim problemi yaşatacak saldırı gibi bir durum karşısında sertifika durum bilgilerine erişim engellemez. Blockchain, merkezi veya dağıtık veri tabanlarına karşı sahip olduğu yüksek erişilebilirlik özelliği sayesinde tek bir noktaya bağlı olmadan her zaman kolay bir şekilde istenilen bilgiye ulaşılabilirlik imkanı sunar. Bu özelliği ile sertifika iptal bilgileri için tek nokta hatası problemine çözüm sağlar. Ayrıca farklı SM'lerin iptal bilgilerinin ortak bir blockchain platformunda tutulması farklı SM iptal bilgilerini kontrol eden bir kullanıcı açısından kontrolü de kolaylaştıracaktır.

6.4. Sertifika İptal Bilgileri İçin Ayrılan Kaynaklar

İstenilen sertifika iptal bilgisinin elde edilmesinde geleneksel yöntemlerin yetersiz kaldığı durumlarla karşılaşılabilir. Bu gibi durumlarda SM yetkilisinden destek istenir. Ulaşılmak istenilen bilgi için üçüncü bir kişiye ihtiyaç duyulması fazla iş gücü sorununu da beraberinde getirir. Sertifika iptal bilgilerine blockchain kullanılarak sürekli, üçüncü kişiye gerek olmadan ve güvenilir bir yöntem kullanılarak erişilebilir.

BÖLÜM 7. METOT / YÖNTEMLER

5070 sayılı Elektronik İmza Yasası'na uygun güvenli elektronik imza, nitelikli elektronik sertifika (NES) kullanılarak oluşturulur (Resmi Gazete, 2004). NES, X.509 standardına uygun olarak üretilir ve bu standartla uyumlu olan web tarayıcılarına, akıllı kartlara, akıllı çubuklara yüklenebilir. Örneğin TCKK ile nitelikli elektronik imza atılması, Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) tarafından NES ve anahtarların, Kart Erişim Cihazı (KEC) aracılığı ile yüklenmesi sonrasında mümkün olmaktadır (Çelik ve Adalier, t.y.).

Blockchain'in dağıtık ve ortak defterler özelliği tek nokta hatası ve SM kesintilerinin giderilmesine karşı etkilidir. Bunun sonucunda tamamıyla izlenebilir bir geçmiş işlem günlüğü tutulmuş olur. Böylece geleneksel AAA yapısındaki sertifika iptal yöntemlerinin sorunlarına da çözüm getirmektedir.

Ek olarak blockchain tabanlı AAA, açık ve sadece yazılabilen işlem günlükleri özelliğiyle doğal olarak Google tarafından önerilen Sertifika Şeffaflığı (Certificate Transparency) özelliğini de sağlamaktadır (Laurie ve diğerleri, 2013).

Sertifika iptal bilgileri için dağıtık uygulama (DApp) tasarlanmıştır. Tasarlanan genel yapı SM'ler, SM kayıt servisi, blockchain ağı, akıllı sözleşme ve bir kullanıcı ön yüzünden oluşmaktadır. Bu çalışma kapsamında uygulamaya alınan dağıtık uygulama, bir kullanıcı ön yüzü ve blockchain üzerinde çalışan, akıllı sözleşmenin oluşturduğu bir arka yüzden oluşmaktadır. SM'lerin oluşturduğu blockchain ağ yönetimi ve SM Kayıt Servisi bu prototip uygulamanın kapsamı dışındadır.

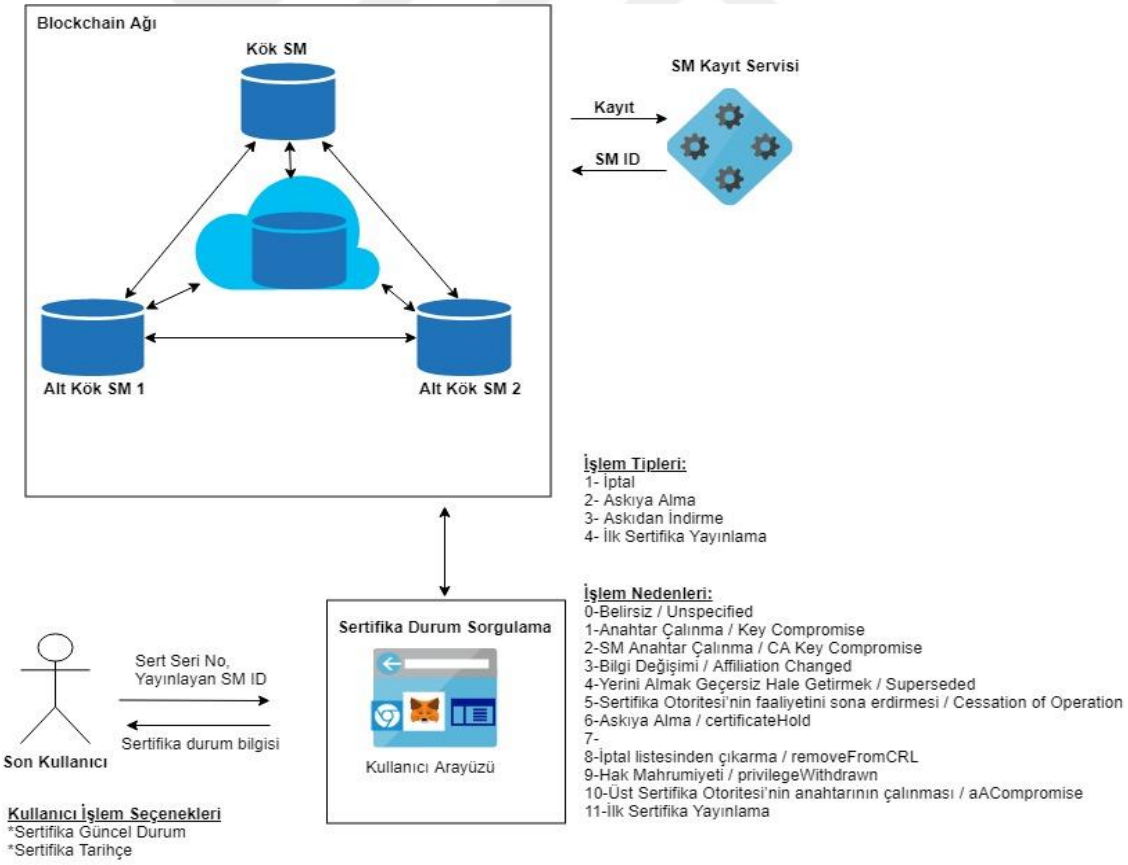
Çalışmanın uygulamalı kısmında blockchain teknolojisi olarak ethereum (Wood, 2014) blockchain platformu tercih edilmiştir. Ethereum'un sağladığı akıllı sözleşmeler sayesinde birçok sektörde devrim yaratacak dijital özellik desteklenmekte ve bunu ise blockchain teknolojisinin sunduğu zaman damgalı ve sonradan değiştirilemez güvenilir bir veri bütünlüğü sağlayarak gerçekleştirmektedir.

7.1. Blockchain Tabanlı Dağıtık Uygulama ile Elektronik Sertifika Durum Bilgilerinin Yönetilmesi

Tasarlanan sistemde yer alan varlıklar SM'ler, SM kayıt servisi, blockchain ağı, akıllı sözleşme, kullanıcı arayüzü ve son kullanıcıdan oluşmaktadır. Sistemde yer alan varlıklar insan veya insan olmayan herhangi bir katılımcıya atıfta bulunabilir.

Tasarlanan dağıtık uygulama için ethereum blockchain ağı üzerinde akıllı sözleşme tarafından kontrol edilen mantıksal iş katmanı ve bu iş katmanıyla etkileşimli çalışan kullanıcı arayüz uygulamasını kapsayan bir prototip üzerinde çalışılmıştır. Sertifika durum verilerinin yönetimi, yetki işlemleri ve izinler blockchain ağındaki akıllı sözleşme ile yönetilmektedir.

AAA yapısındaki sertifikalandırma sürecine uygun olarak blockchain teknolojisinin entegre edilmesi için Şekil 7.1.'deki gibi genel bir bakış açısı tasarlanmıştır.



Şekil 7.1. Genel sistem altyapısı

Sisteme genel bir bakış açısı kazandırmak için tasarlanan yapı bir kök ve iki alt kök sertifika makamından oluşacak şekilde planlanmıştır. Fakat ihtiyaca göre daha karmaşık yapılarla da uygulama gerçekleştirilebilir. Geleneksel AAA yapısında olduğu gibi kök SM'nin kendi sertifikasını kendisinin imzalayarak oluşturmasından sonra alt kök SM sertifikaları kök SM tarafından imzalanarak oluşturulur. Alt kök SM'ler ise kullanıcı sertifikalarını yayınlar. Hem kök hem de alt kök SM sertifikaları oluşturulurken SM kayıt servisi tetiklenir. Kök SM için sertifika oluşturulurken SM kayıt servisinde özel SM ID numarası üretilir ve blockchain akıllı sözleşmesi kök SM sahipliğinde oluşturulur. Alt kök SM'ler için sertifika oluşturulurken ise her SM için kayıt servisinden SM ID edinilir.

Sertifikaların ilk yayınlanması, iptal edilmesi, askıya alma ve askıdan indirme işlemleri için akıllı sözleşmeye gönderilecek alanlar SM tarafından blockchain ağına iletilir. İlk defa bir sertifika yayınlanırken sertifika seri numarası, konu ve sertifika yayınlanma zaman bilgisi blockchain akıllı sözleşme hesabına gönderilir. İlgili SM yayınladığı sertifikalarda iptal, askıya alma ya da askıdan indirme gibi sertifika güncelleme işlemlerini gerçekleştirirken sertifika seri numarası, işlem tipi ve işlem nedeni bilgilerini akıllı sözleşme hesabına iletir. İşlem yapan varlığın SM'ye ait olup olmadığı akıllı sözleşmede tanımlanan SM hesap adresleri kontrol edilerek gerçekleştirilir. İşlem yapan varlığın SM olduğu tespit edildikten sonra ilgili işlemler blockchainin yapısı gereği değiştirilemez bir şekilde kaydedilerek saklanır. Sözleşme sahibi olan kök SM tarafından farklı nedenlerle SM'lerin hesap bilgileri silinebilir veya yetkili yeni bir SM hesabı eklenebilir. Bir SM hesabı, sözleşme sahibi tarafından silinse bile blockchainde geriye dönük işlemler silinemediğinden SM'nin yaşamı boyunca işlem yaptığı tüm sertifika durum bilgilerine ulaşılabilir.

Son kullanıcılar web arayüzü uygulamasında sertifika güncel durum bilgisi ve sertifika tarihçesi sorgulama gibi iki farklı seçeneğe sahiptir. Sertifika iptal bilgileri, SİL yönteminde olduğu gibi tüm kullanıcılara açıktır. Prototip uygulamada, son kullanıcılar işlemlerini kullanıcı arayüzü yardımıyla tarayıcı eklentisi matamask cüzdan hesaplarını kullanarak gerçekleştirmektedir. Kullanıcı, sorgulamak istediği sertifikanın seri numarası ve yayınlayan SM ID numarası ile ilgili sertifikanın güncel durum bilgisini veya sertifikanın yayınlanmasından itibaren tüm tarihçesini görüntüleyebilir. Sertifika güncel durum bilgisi için sertifika seri numarası ve yayınlayan SM ID numarasına

karşılık gelen blockchaindeki en güncel veri alınır. Sertifika tarihçesi için sertifika seri numarası ve yayınlayan SM ID'ye karşılık gelen blockchain ağındaki ilgili tüm bloklar taranarak ilgili sertifika verileri kullanıcı arayüzünde geçmişten günümüze doğru listelenir.

7.2. Sertifika Makamı (SM) , Sertifikalar ve SM Kayıt Servisi

AAA tabanlı sistemlerde kök SM'ler kendi kendisinin sertifikasını imzalar ve son derece güvenilir olduğu kabul edilir. Alt kök SM sertifikaları kök SM tarafından imzalanarak yayınlanır. Kullanıcı sertifikaları ise alt kök SM'ler tarafından imzalanarak yayınlanır ve başka bir sertifikayı imzalama özelliği bulunmaz. Sertifikalandırma sürecindeki bu hiyerarşik yapı için bu çalışmada bir değişiklik bulunmamaktadır.

Tasarlanan yapıya göre hem kök hem de alt kök SM sertifikaları oluşturulurken SM kayıt servisi tetiklenir. Kök SM için sertifika oluşturulurken SM kayıt servisinde özel SM ID numarası üretilir ve blockchain akıllı sözleşmesi oluşturularak kök SM'nin ethereum hesap adresi akıllı sözleşme sahibi olarak kaydedilir. Alt kök SM'ler için sertifika oluşturulurken kayıt servisinden her SM için özel SM ID edinilir. Bu şekilde SM sertifikasının bir servis ile kaydedilmesi Google'ın Sertifika Şeffaflığı projesinde SSL sertifikaları için yapılan kayıt işlemine benzetilebilir (Laurie ve diğerleri, 2013). SM ID değeri, sadece SM sertifikalarında tutulmaktadır. SM'ler kendilerine özel SM ID numarasıyla diğer SM'lerden farklılaşırken SM'lerden yayınlanacak her bir sertifika, yayınlayan SM ID değeri ile oluşturulduğu SM'nin izini taşır.

Tasarlanan X.509 hibrit sertifika, Tablo 7.1.'deki gibi hiyerarşik bir yapıya sahiptir. Geleneksel AAA yapısında her SM, kendi imzalayarak yayınladığı sertifikanın/sertifikaların iptal bilgisinden sorumludur. Tasarlanan yapıda yine her SM kendi imzaladığı sertifikanın iptal bilgisini yayınlar. Farklı SM'lerin yayınladığı sertifikalar aynı sertifika seri numarasına sahip olabilirler. Aynı seri numarasına sahip sertifikalar, her SM'nin kendine özel bir ID'si olduğundan yayınlayan SM ID numarasıyla farklılaşarak ayırt edilebilirler. Özetle yayınlayan SM ID ve sertifika seri numarası değerleri tek bir sertifikayı işaret eder. SM'ler sertifikaların durum bilgilerinin kayıt altına alınması için yayınlama, iptal, askıya alma ve askıdan indirme bilgilerini blockchain ağına gönderir. Dağıtık defterlerde, yayınlayan SM ID ve sertifika seri

numarası birlikte tutulur. Böylece hangi SM tarafından hangi sertifikanın durum bilgisinin güncellendiği bilgisine kolaylıkla ulaşılabilir.

Tablo 7.1. Blockchain hibrit sertifika hiyerarşisi

Sertifika	Sertifika Seri No	Yayınlayan SM ID	SM ID	Akıllı Sözleşme
Kök SM	Kök Sertifika Seri No	Kök SM ID	Kök SM ID	0x1234xxxx
Alt Kök SM	Alt Kök Sertifika Seri No	Kök SM ID	Alt Kök SM ID	0x1234xxxx
Son Kullanıcı	Son Kullanıcı Sertifika Seri No	Alt Kök SM ID	-	0x1234xxxx

Bir X.509 v3 standardına sahip sertifikanın uzantılar alanına ihtiyaç doğrultusunda veri eklenmesi mümkündür. Nitelikli elektronik sertifikalar, X.509 v3 standartlarına uygun olarak 5070 sayılı Kanunun 9 uncu maddesinde belirtilen niteliklere göre üretilirler (TUBITAK Kamu Sertifikasyon Merkezi, 2018). Bu çalışmada sertifika durumlarının blockchain sisteminde tutulabilmesi için X.509 v3 sertifikalarının uzantılar alanına aşağıdaki ek alanlar eklenerek Şekil 3'teki hibrit sertifika elde edilmiştir:

- Akıllı Sözleşme: Blockchain ağındaki akıllı sözleşme adresini tutar. Bu adres kullanılarak blockchain ağındaki akıllı sözleşme ile etkileşimde bulunulur.
- SM ID: SM kayıt servisi tarafından her SM'ye özel bir ID numarası sadece SM sertifikalarına verilir.
- Yayınlayan SM ID: Her sertifikanın hangi SM tarafından yayınlandığını belirtir.

Sertifikaların ilk yayınlanması, iptal, askıya alma ve askıdan indirme gibi güncelleme işlemlerinde bölüm 6.3'de detayları belirtilen alanlar SM tarafından blockchaine gönderilir.

X.509 v3 standart sertifika:

Sürüm
Seri No
İmza Algoritması
İmza Karma Algoritması
Geçerlilik Başlangıcı
Geçerlilik Sonu
Sertifikayı Veren
Konu
Ortak Anahtar
Ortak Anahtar Parametreleri
Uzantılar
İmza

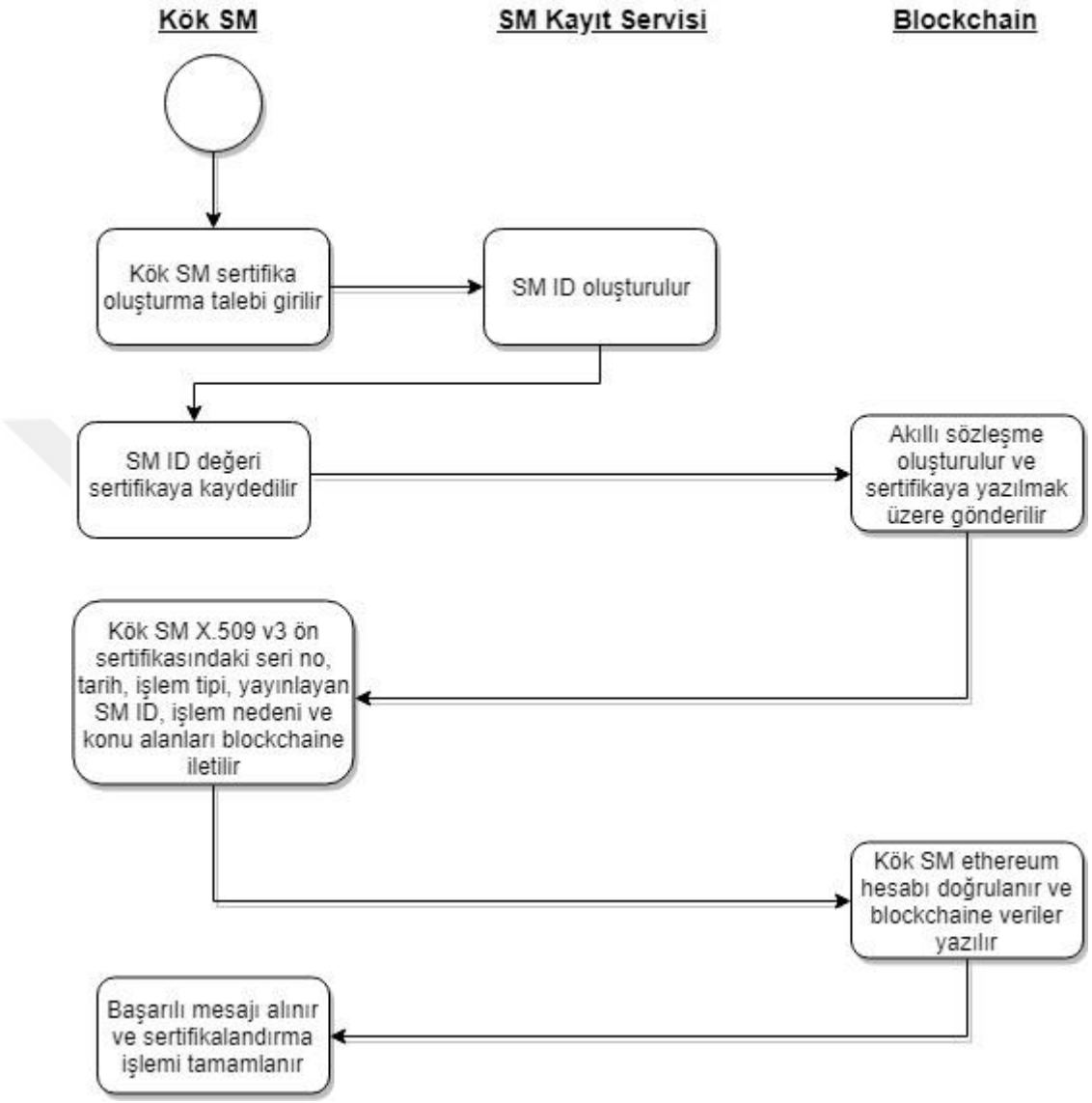
X.509 v3 hibrit sertifika:

Sürüm
Seri No
İmza Algoritması
İmza Karma Algoritması
Geçerlilik Başlangıcı
Geçerlilik Sonu
Sertifikayı Veren
Konu
Ortak Anahtar
Ortak Anahtar Parametreleri
Uzantılar
Yetkili Anahtar Tanımlayıcısı
Konu Anahtar Tanımlayıcısı
Sertifika İlkeleri
Temel Kısıtlamalar
CRL Dağıtım Noktaları
Yetkili Bilgi Erişimi
Yetkili Sertifika Bildirimleri
…
Akılı Sözleşme
SM ID
Yayınlayan SM ID
İmza

Şekil 7.2. Standart ve önerilen hibrit X.509 v3 sertifikaları

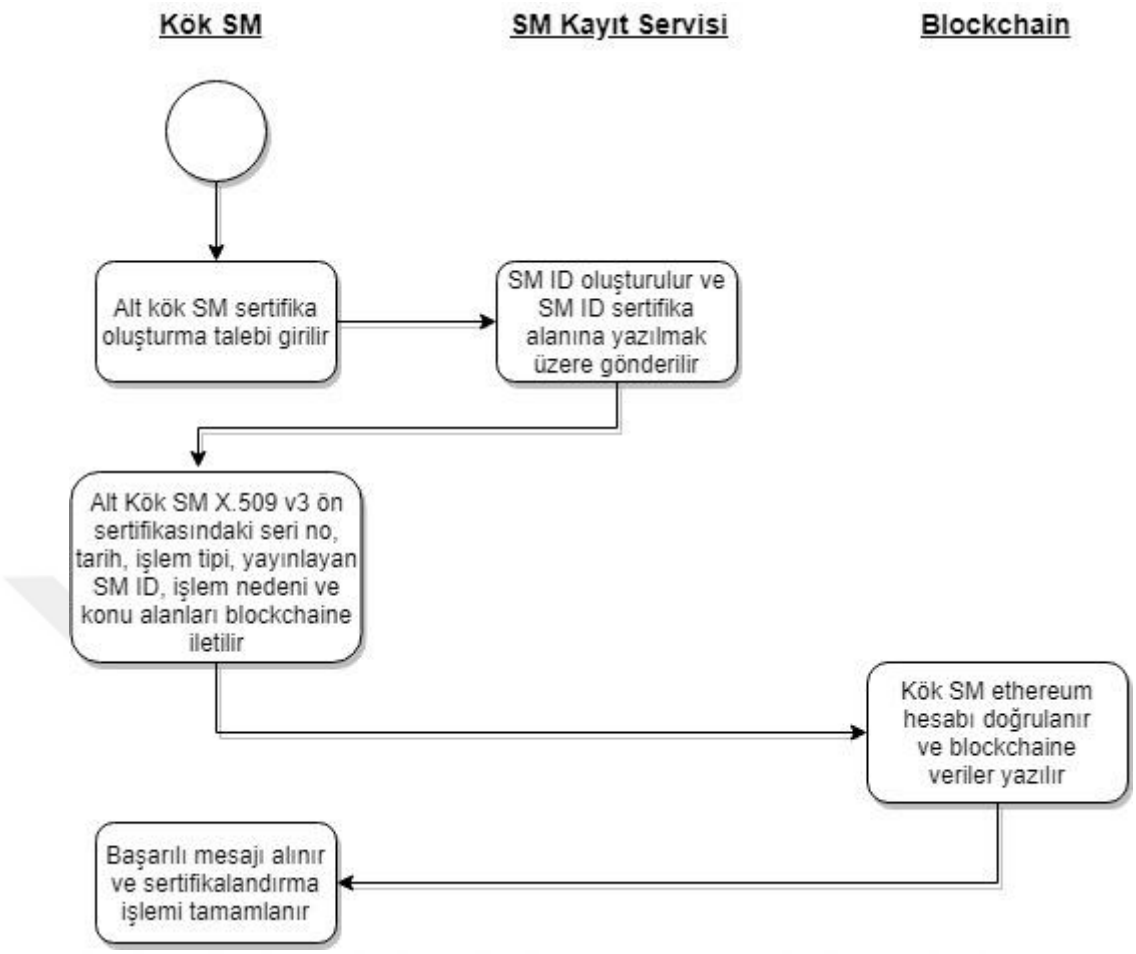
Kök SM için sertifika oluşturulurken SM kayıt servisi tetiklenir ve kök SM'ye özel bir SM ID oluşturulur. Ön sertifikaya SM ID kaydedildikten sonra ethereum akıllı sözleşmesi kök SM sahipliğinde oluşturulur ve akıllı sözleşme adresi X.509 v3 sertifikasındaki genişletilmiş alana kaydedilir. Ön sertifikadaki ilgili alanlar blockchain ağına gönderilir ve akıllı sözleşmedeki yetkili SM kök hesabı doğrulanarak blockchaine

yazılır. Başarılı işlem sonrasında sertifikalandırma işlemi tamamlanır. Şekil 7.3.'de kök SM sertifikasının oluşturulma akışı yer almaktadır.



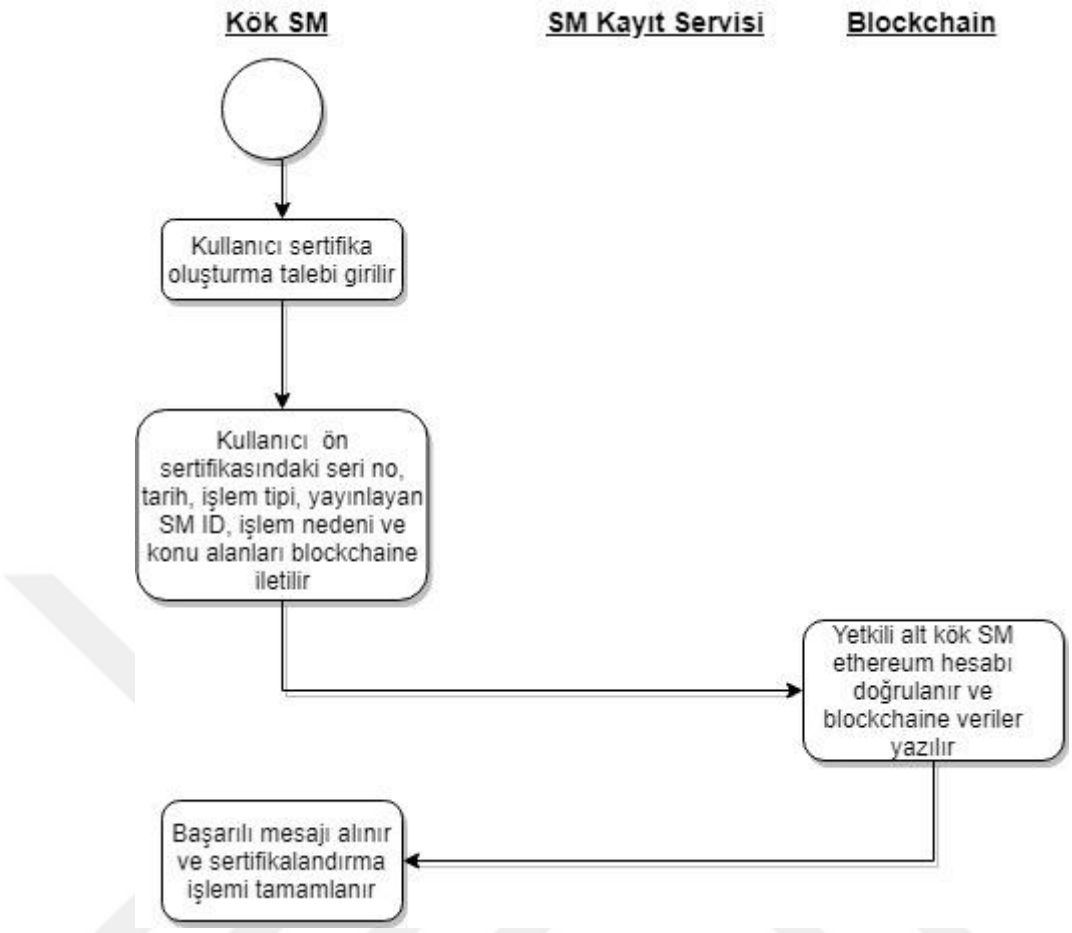
Şekil 7.3. Kök SM sertifikalandırma akışı

Alt kök SM oluşturmak için Şekil 7.4.'teki gibi kök SM'ye benzer bir akış izlenir. İki akış arasındaki fark, alt SM sertifikası oluşturulurken yeni bir akıllı sözleşme oluşturulmamasıdır.



Şekil 7.4. Alt kök SM sertifikalandırma akışı

Kullanıcı sertifikası oluşturulma akışı Şekil 7.5.'te yer almaktadır. Kullanıcı sertifikası oluşturulurken SM kayıt servisi kullanılmaz. Sertifika talebi ile bir ön sertifika oluşur ve ön sertifikadaki bilgiler blockchaine iletilir. Blockchain'de sertifikalandırma yapan SM'nin hesabı doğrulanır ve kullanıcı sertifika verileri blockchainde kaydedilir. Başarılı işlem sonrasında kullanıcı sertifikası sertifikalandırma işlemi tamamlanır.



Şekil 7.5. Kullanıcı sertifikalandırma akışı

7.3. Ethereum Blockchain Ağı

Dağıtık prototip uygulamada ethereum blockchain teknolojisi ile bir blockchain test ağında akıllı sözleşmenin olduğu iş katmanı geliştirilmiştir. Tasarlanan yapıdaki üç SM, blockchain ağına veri göndererek yazma hakkına sahipken kullanıcılar blockchain ağındaki verileri okuma hakkına sahiptir.

Seçilecek blockchain ağ türü ihtiyaca göre farklı şekillerde kurgulanabilir. Bu çalışma için planlanan blockchain ağında sadece yetkili SM düğümlerinin konsensüs sürecine katılması önemli olduğu için blockchain türünün seçimi yapılırken izne tabi (permissioned) bir konsensüs yapısının olması önemlidir.

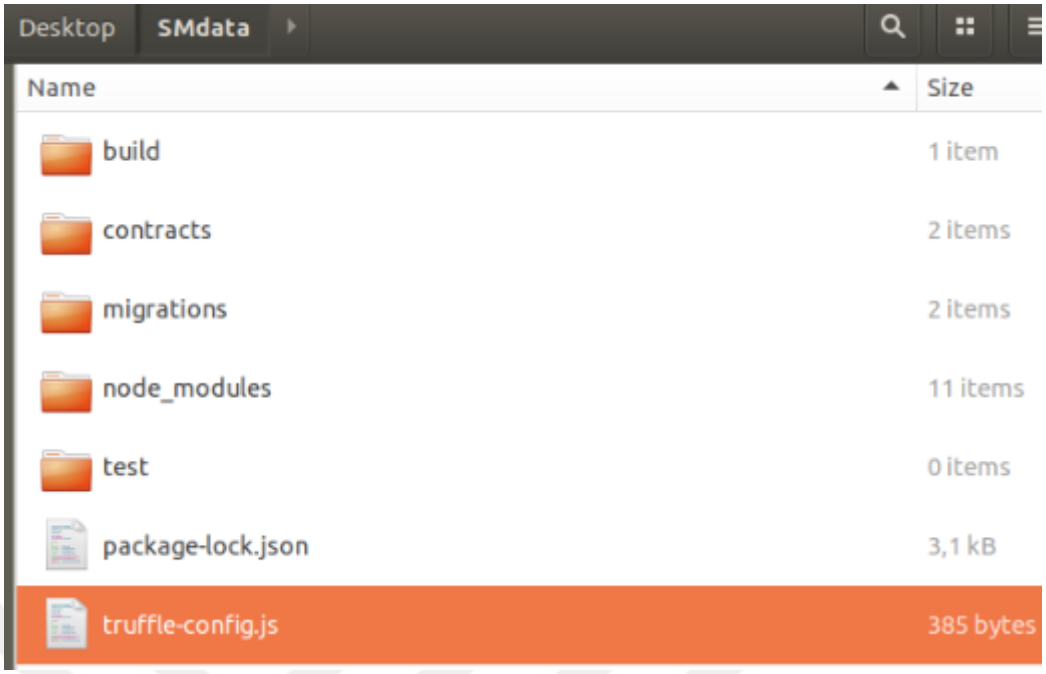
Konsensüs yapısının izne tabi olduğu durumlarda blockchain ağ tipi, bir özel kuruluş içerisinde veya birkaç kuruluşun bir araya gelerek oluşturduğu şekilde ihtiyaç

doğrultusunda tasarlanabilir. Bilgi gizliliğinin önemli olduğu ve tek bir kuruluş içerisinde kalması gerektiği durumlarda özel ağ seçimi daha uygundur. Buna karşılık mutabakat sürecinde birden fazla organizasyonu içeren ortak bir ağ yapısı için ise konsorsiyum blockchain tercih edilebilir. Her ikisinin de farklı avantaj ve dezavantajları bulunmaktadır. Prototip için kurgulanan yapı, bir organizasyona ait bir kök SM ve iki alt SM'den oluşmaktadır. Fakat birden fazla organizasyondaki SM'lerin birbiri ile etkileşim içerisinde olduğu bir yapı da tasarlanabilir.

Bu çalışmada blockchain ağının her bir düğümü sisteme kayıtlı yetkili SM'leri temsil etmektedir. Sisteme katılmak isteyen SM'ler yetkili makamlardan izin aldıktan sonra yetkili makam tarafından ağa katılım için gerekli olan yapılandırma ayarlarının yapılması sonrasında ağa eklenerek bir düğüm haline gelebilirler.

Ethereum blockchain test ağını kullanabilmek için gerekli ağ yapılandırması Truffle geliştirme ortamı aracılığıyla gerçekleştirilmiştir. Dünya standartlarında bir geliştirme ortamı olan Truffle ile ethereum özel/açık blockchain ağları yönetilebilir, akıllı sözleşmeler geliştirebilir, sözleşmeler derlenerek ağa yüklenebilir ve test edilebilir. Ethereum, geliştirmeciler için üç farklı test ağı sunmaktadır. Bu test ağları Ropsten, Kovan ve Rinkeby'dir. Ropsten, iş kanıtı (PoW) konsensüs algoritması kullanırken Kovan ve Rinkeby, otorite ispatı (PoA) algoritması kullanmaktadır. PoA algoritması kullanılması, blokların iyi bilinen ve güvenilir topluluk üyeleri tarafından imzalandığı anlamına gelir. PoA, bilgi gizliliğinin önemli olduğu kurumların özel bir ağda blockchain teknolojisinden faydalanmalarına imkan sağlar. Bu sayede saldırganların ağdaki madencilik gücünü ele geçirmelerini önlenir. Prototip uygulamada ethereum test ağı olarak küresel şekilde çalışan Rinkeby test ağı tercih edilmiştir.

Uygulama için Truffle geliştirme ortamı kullanılarak SMdata projesi oluşturulmuş ve Şekil 7.6.'da projenin klasör yapısı gösterilmiştir.



Şekil 7.6. Proje dosyaları

Uygulama için gerekli olan sözleşme “contracts” klasörü altında yazılarak proje dizinine kaydedilmiştir. Rinkeby test ağını kullanabilmek için Infura’dan yararlanılmıştır. Infura, ethereum blockchain üzerinde dağıtık uygulama oluşturmak için güvenilir, ölçeklenebilir ve kullanımı kolay API'ler sağlar. Infura, bir düğüm kurmadan ve bu düğümü korumak zorunda kalmadan dağıtık bir Ethereum ağına güvenilir bir şekilde mesaj alınıp gönderme imkanı sağlar. Proje dizininde Rinkeby test ağına bağlanmak için gerekli yapılandırma truffle-config.js dosyasının içerisinde yapılmıştır. Rinkeby test ağında PoA algoritması gereği kimlikleri doğrulanmış imzalayıcı düğümler bulunmaktadır (“Rinkeby: Ethereum Testnet”, 2019). Rinkeby küresel test ağı sayesinde akıllı sözleşmeye ait işlemler izlenebilir, sözleşmenin kaynak kodu görüntülenebilir, sözleşme içerisindeki bilgiler okunabilir, internet tarayıcısı üzerinden metamask cüzdan hesabı ile bağlanarak sözleşmedeki yetkiler dahilinde işlemler oluşturulabilir ve olay günlükleri sayesinde sözleşme eylemleri takip edilebilir.

Ethereum test ağları, işlemler için gerçek paralar kullanılmadan geliştirmecilerin kodlarını ve uygulamalarını test etmelerine imkan sağlar. Ethereum ana ağı ve test ağları arasındaki tek fark, farklı ağlarda yönetiliyor olmalarıdır. Rinkeby test ağının

kullandığı PoA algoritması ile ethereum konsorsiyum veya özel ağda SM'lerin yetkili ağ düğümü olduğu bir yapı oluşturulabilir.

7.4. Akıllı Sözleşme

Uygulamanın mantıksal iş katmanındaki akıllı sözleşme Solidity programlama dili kullanılarak yazılmıştır. Solidity, ethereum blockchain teknolojisinde akıllı sözleşmelerin yazılması için kullanılan en yaygın dildir. Akıllı sözleşmeler için blockchain üzerinde çalışan kodlar da denebilir. Bu kodlar ağdaki tüm düğümler tarafından çalıştırılır (Murat, 2018).

Yetkili SM hesaplarının sertifika yayınlaması ve sertifika durum güncellemeleri yapmaları, kullanıcıların sertifika durum bilgilerini sorgulaması, yetkili SM hesaplarının blockchainde eklenmesi ve silinmesi gibi akışlar akıllı sözleşmede farklı metotlarla programlanmıştır. Akıllı sözleşmedeki metotlar farklı yetkideki varlıklar tarafından çalıştırılabilmektedir. Örneğin akıllı sözleşmede tanımlanmış sertifika yayınlama ve güncelleme metodunu sadece sözleşmedeki ethereum hesap adresi doğrulanan SM'ler çalıştırabilir. İşlem blockchainde başarılı bir şekilde işlendikten sonra kullanıcı sertifikası yayınlanma işlemi tamamlanmış olur. Akıllı sözleşme kaynak kodundaki metotların bir kısmı Şekil 7.7.'de gösterilmiştir.

Smart Contract

```
124
134     function issueCertificate(
135         uint256 certificateID_,
136         string memory domainName_,
137         uint256 issueDate_
138         ) onlyCA public returns(bool) {
163
164
165     function updateCertificate(
166         uint256 certificateID_,
167         uint256 processType_,
168         uint256 processReason_
169         ) onlyCA public returns(bool) {
190
191
192     function lookUpCertificate(
193     uint256 certificateID_,
194     string memory _caID
195     ) public view returns(uint256, string memory, string memory, uint256, uint256, uint256){
205
206
207     function seeALLCA() public view returns (address[] memory){
210
211
```

Şekil 7.7. Akıllı sözleşme kaynak kodu örneği

Blockchain dağıtık defterlerinde sertifikalar için saklanan alanlar Tablo 7.2.'de yer almaktadır.

Tablo 7.2. Sertifika iptal bilgileri için dağıtık defterlerde saklanan alanlar

Sertifika Seri No	Tarih	İşlem Tipi	Yayınlayan SM ID	İşlem Nedeni	Konu

Tablo 7.2.'de yer alan verilerin detayları aşağıdaki gibidir:

- Sertifika Seri No: İşlem yapılan sertifikanın seri numarası.
- Tarih: İşlem tarihi.
- İşlem Tipi: Dört farklı işlem tipi aşağıdaki sayısal gösterimle tutulur.

1→İptal
2→Askıya Alma
3→Askıdan İndirme
4→İlk Sertifika Yayınlama

- Yayınlayan SM ID: Sertifikayı yayınlayan SM'ye özel SM ID.
- İşlem Nedeni: Bir sertifikanın geçersiz duruma gelmesinin farklı sebepleri olabilir. Uygulamada RFC 5280 standardında yer alan sertifika iptal nedenleri ve kodları baz alınmıştır (Boeyen ve diğerleri, 2008). RFC'de belirtilen iptal nedenlerine ek olarak ilk sertifika yayınlama için bu çalışmaya özel bir işlem nedeni eklenmiştir.

0→Belirsiz / Unspecified
1→Anahtar Çalınma / Key Compromise
2→SM Anahtar Çalınma / CA Key Compromise
3→Bilgi Değişimi / Affiliation Changed
4→Yerini Almak Geçersiz Hale Getirmek / Superseded
5→Sertifika Otoritesi'nin faaliyetini sona erdirmesi / Cessation of Operation
6→Askıya Alma / certificateHold
7→- (kullanılmamakta)
8→İptal listesinden çıkarma / removeFromCRL
9→Hak Mahrumiyeti / privilegeWithdrawn
10→Üst Sertifika Otoritesi'nin anahtarının çalınması / aACompromise

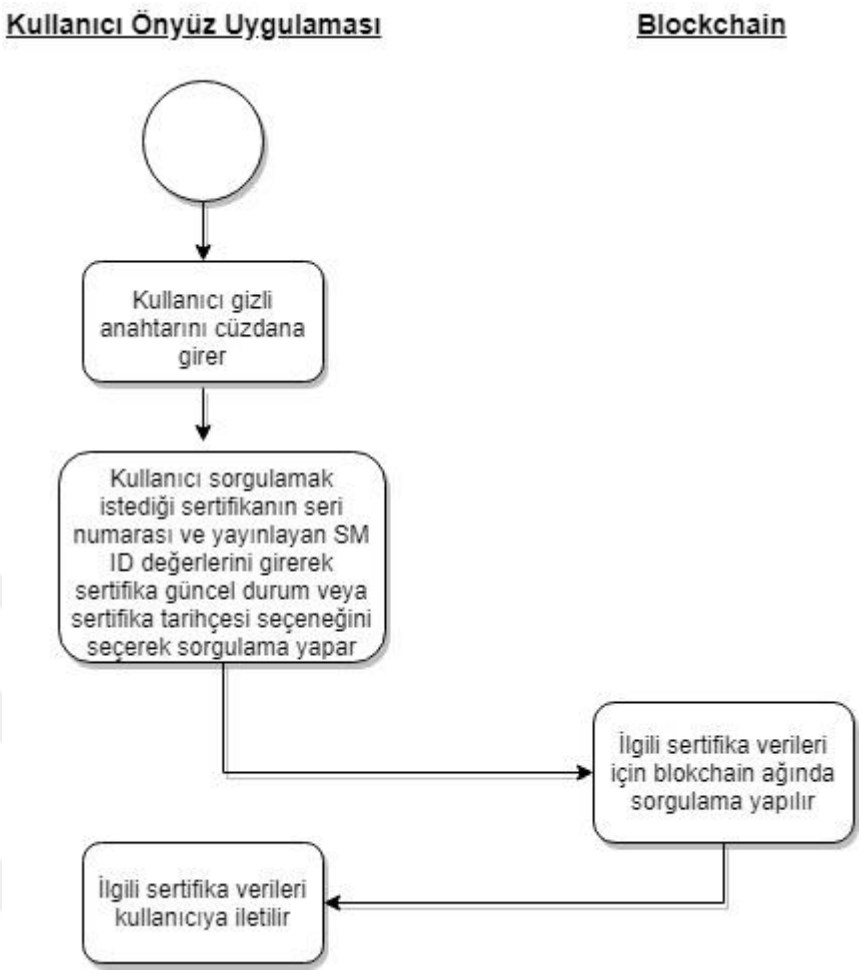
11→İlk Sertifika Yayınlama / Initial Certificate Issue

- Konu: NES'in verileceği kişinin ayırt edilebilir adını içerir. RFC 3739 (Santesson ve diğerleri, 2004) NES standardındaki şartlara uygun şekilde doldurulmalıdır. Bu şartlara uyulmasının yanında 5070 Elektronik İmza Kanunu'na göre commonName, serialNumber ve C niteliklerinin bulunması zorunludur (Resmi Gazete, 2004).

7.5. Sertifika Durum Bilgisi için Kullanıcı Arayüz Uygulaması

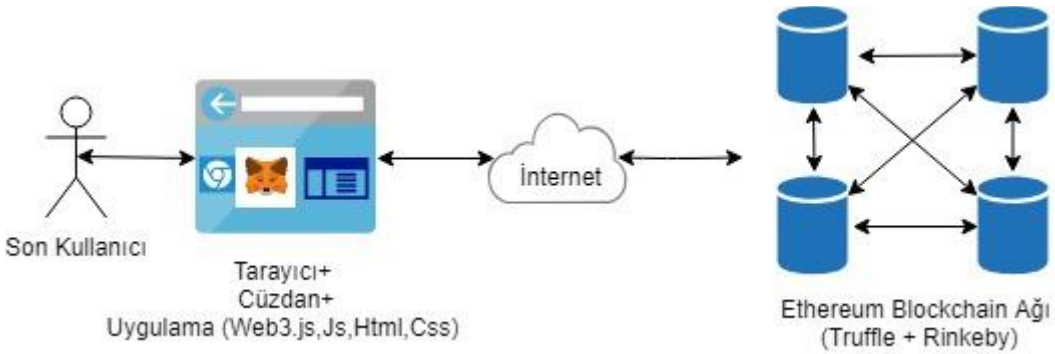
Bu çalışmada ethereum blockchain platformunda Solidity akıllı sözleşme programlama dili kullanılarak tasarlanan iş mantığını içeren akıllı sözleşme ile web arayüzünü kapsayan bir prototip dağıtık uygulama geliştirilmiştir. Blockchain ağı üzerindeki akıllı sözleşme ile etkileşimli çalışan web arayüzü arasındaki iletişim web3.js kütüphanesi ile sağlanmıştır. Bu arayüz genel sistem yapısında son kullanıcılar tarafından kullanılmaktadır. Aynı zamanda akıllı sözleşmede tasarlanan iş akışlarının istenildiği gibi sonuç verdiğinin kontrolü için test amacı ile de kullanılmıştır.

Arayüzde yetki kontrolünün yapılabilmesi için kullanıcılar tarayıcı eklentisi olan metamask cüzdana gizli anahtarlarını girdikten sonra oturum açmaktadır. Metamask cüzdan, kolay arayüzü sayesinde ethereum ana ağı veya test ağı üzerinde işlem yapılmasına olanak sağlayan bir internet tarayıcı eklentisidir. Bu çalışmada metamask cüzdan hesabı, Rinkeby test ağına bağlanılarak kullanılmaktadır. Akıllı sözleşmede belirlenen yetkiler dahilinde işlem yapan kullanıcıların etkileşimleri web3.js kütüphanesi ile Rinkeby test ağına iletilir. İlgili sözleşme metodunun cevabı arayüze döner. Kullanıcı veri okuma akışı şekil 7.8.'de gösterilmiştir.



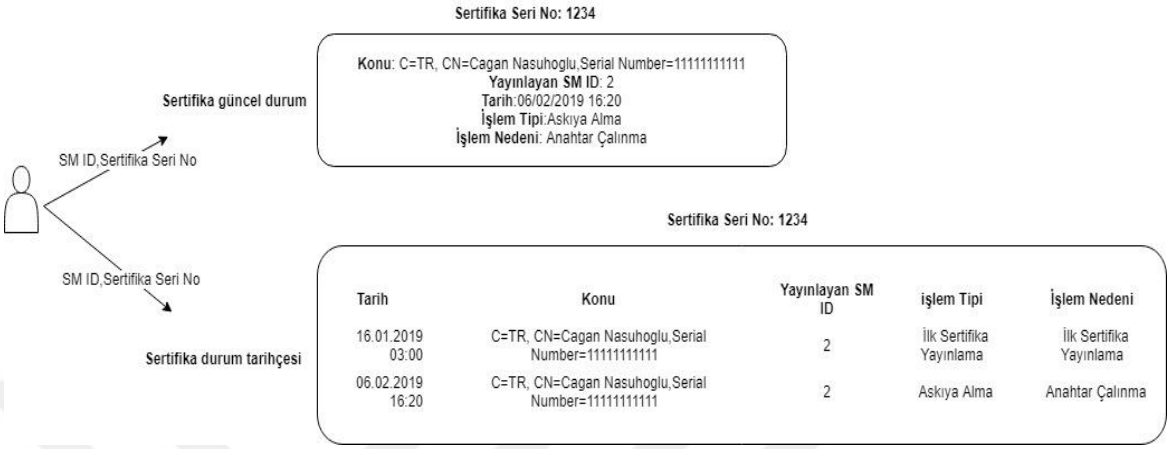
Şekil 7.8. Kullanıcı veri okuma akışı

Dağıtık uygulama mimarisinin görselleştirildiği çizim Şekil 7.9.'da verilmiştir.



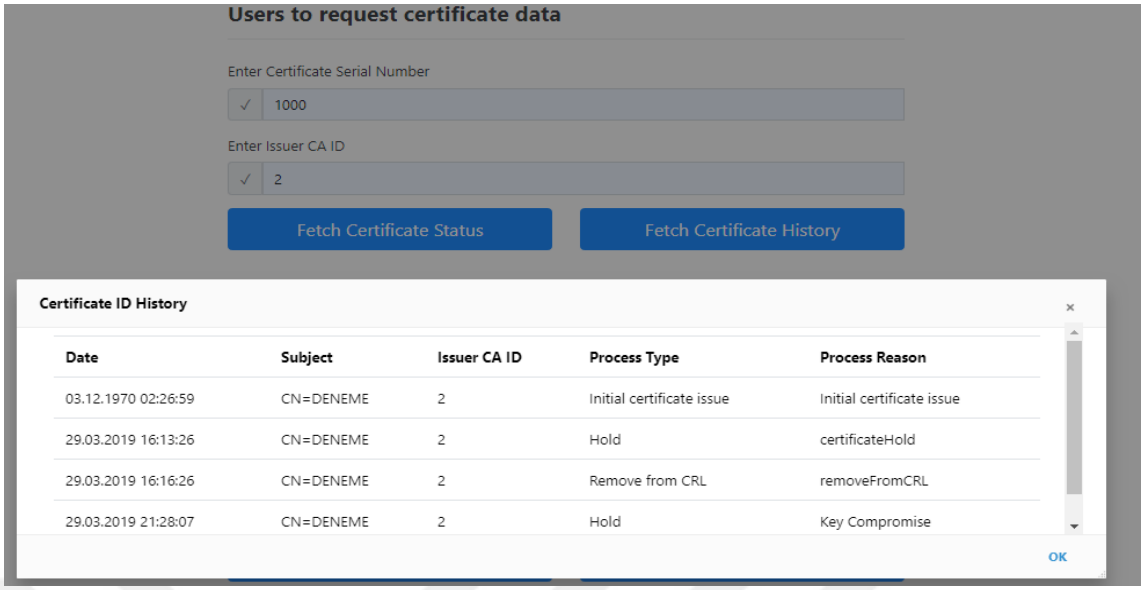
Şekil 7.9. Dağıtık uygulama mimarisi

Son kullanıcılar, Şekil 7.10.'daki gibi sertifika güncel durum bilgisi ve sertifika tarihçesi sorgulama gibi dağıtık defterden sadece okuma yapabilecekleri iki farklı seçeneğe sahiptir.



Şekil 7.10. Web arayüzünde sertifika güncel durum ve sertifika tarihçesi sorgulama örneklerinin gösterimi.

Kullanıcı, sorgulamak istediği sertifikayı belirten sertifika seri numarası ve yayınlayan SM ID verisi ile sertifikanın güncel durum bilgisini veya sertifikanın yayınlanmasından itibaren tüm tarihçesini görüntüleyebilir. Sertifikanın güncel durum bilgisi için sertifika seri numarası ve yayınlayan SM ID değerlerine karşılık gelen blockchaindeki en güncel veri alınır. Sertifika tarihçesi için ise sertifika seri numarası ve yayınlayan SM ID değerlerine karşılık gelen blockchain ağındaki ilgili tüm bloklar taranarak aranan sertifika verileri geçmişten günümüze doğru kullanıcı arayüzünde Şekil 7.11.'deki gibi listelenir.



Şekil 7.11. Kullanıcı arayüzünde sertifika tarihçe sorgulama örneği

BÖLÜM 8. TARTIŞMA VE SONUÇ

Çalışma kapsamında blockchain teknolojisinin avantajları, kullanım alanları, farklı blockchain platformları hakkında hem kapsamlı bir araştırma yapılarak hem de konu ile ilgili çeşitli etkinliklere katılarak bilgi toplanmıştır. Bu teknolojinin geleneksel Açık Anahtar Altyapısı sistemlerinde gelişmeye ihtiyaç duyulan alanlar için sağlayabileceği faydalar düşünülmüştür. Araştırmaların sonucunda sertifika iptal bilgilerinin sorunları üzerinde durulmuş ve mevcut problemler için blockchain teknolojisinin fayda sağlayabileceği ön görülmüştür.

Yüksek güvenlik gerektiren durumlarda çevrimiçi yöntemlerin kullanılması olası yanlış işlemlerin engellenmesi adına önemlidir. Bu çalışmada geleneksel AAA sistemlerinin tek nokta hatası problemini gidererek elektronik sertifikaların geçmiş günlüklerine güvenilir bir çevrimiçi yöntemle kolay erişilebilirlik sağlanabilmesi üzerine çalışılmıştır.

Elektronik imza, Nitelikli Elektronik Sertifika (NES) kullanılarak oluşturulur. Sertifikalar X.509 standardına uygun olarak üretilir ve bu standartla uyumlu olan akıllı kartlara, akıllı çubuklara yüklenebilir. Bu çalışmada mevcut AAA yapısındaki sertifika durum bilgileri için yaşanan sorunlara bir hibrit X.509 v3 sertifika yapısı oluşturularak blockchain teknolojisi ile çözüm aranmıştır. Hibrit sertifika yapısı, sertifika hiyerarşisi ve sertifika durum bilgisi için blockchainde ihtiyaç duyulacak minimal bilgiler gözetilerek planlanmıştır. Çalışmada, AAA yapısındaki sertifikalandırma sürecine uygun olarak blockchain teknolojisinin entegre edilmesi için genel bir bakış açısı tasarlanmıştır.

Çalışmanın uygulamalı kısmında kullanıcı arayüzü aracılığıyla elektronik sertifikaların durum bilgilerine sürekli ve kolay erişim sağlanabilecek blockchain ile etkileşimde bulunan bir prototip dağıtık uygulama geliştirilmiştir. Bu dağıtık uygulama ile hem

sertifikaların anlık durum bilgilerine, hem de geçmişe dönük bilgilerine ulaşılabilmektedir.

8.1. Elde Edilen Sonuçlar

Blockchain teknolojisi doğası gereği mevcut sisteme göre yüksek kayıt bütünlüğü, erişilebilirlik ve hata toleransı üstünlüğü sağlamaktadır. Bu özellikleri ile sertifika iptal durumları bazında da birbirinden farklı sorunlara çözüm sağlamıştır.

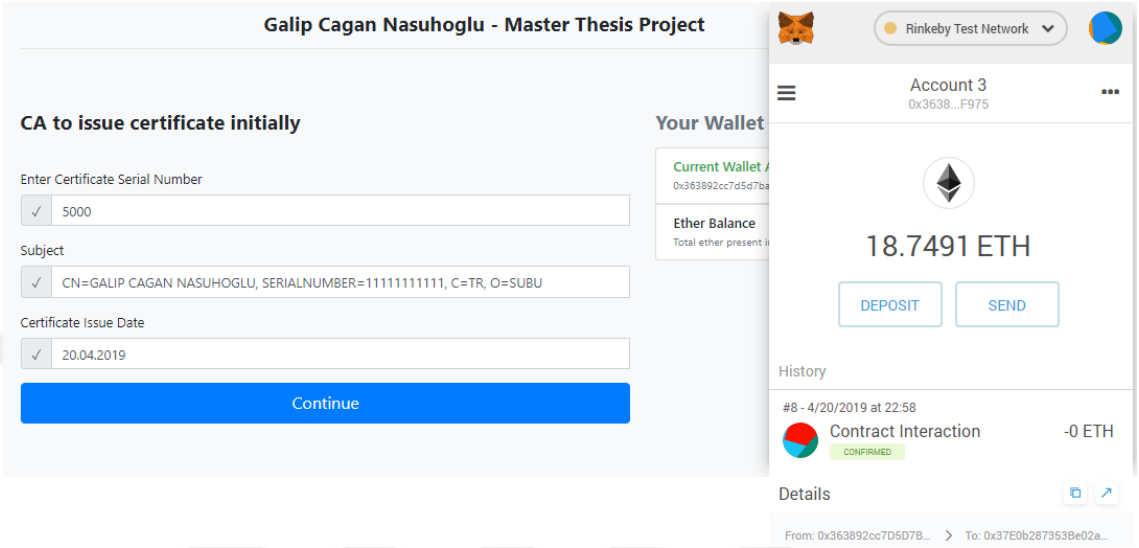
Blockchain, merkezi veya dağıtık veri tabanlarına karşı sahip olduğu yüksek erişilebilirlik özelliği sayesinde merkeziyetçi yapıdan uzak olarak her zaman kolay bir şekilde istenilen bilgiye ulaşım imkanı sunar. Blockchain'in dağıtık defter özelliği sayesinde ağ üzerindeki SM düğümlerinin hepsinde aynı bilgiler tutulur. Bu sayede bir SM'nin yayınladığı sertifika durum bilgisi diğer yetkili SM düğümlerinde de tutulur. Bu özelliği ile mevcut yapıdaki sertifika iptal bilgileri için tek nokta hatası (SPoF) problemine çözüm sağlamıştır.

Elektronik sertifikaların, klasik SM tabanlı sertifika iptal kontrolü yapısına alternatif bir yöntem olarak blockchain tabanlı sertifika durum kontrolü yapılabilecektir. Diğer bir ifade ile X.509 sertifika yapısı korunarak sertifika durum bilgisi için alternatif bir yöntem sağlanmıştır.

Geçmiş bir zaman dilimi için sertifika iptal bilgisinin elde edilmesinde geleneksel yöntemlerin yetersiz kaldığı durumlarla karşılaşılabilir. Bu gibi durumlarda SM yetkilisinden destek istenir. Ulaşılmak istenilen bilgi için üçüncü bir kişiye ihtiyaç duyulması fazla iş gücü ihtiyacını beraberinde getirir. Bu çalışmada sertifika durum tarihçesine ait bilgilere blockchain kullanılarak sürekli, üçüncü kişiye gerek olmadan ve güvenilir bir yöntem kullanılarak erişme imkanı sunulmuştur.

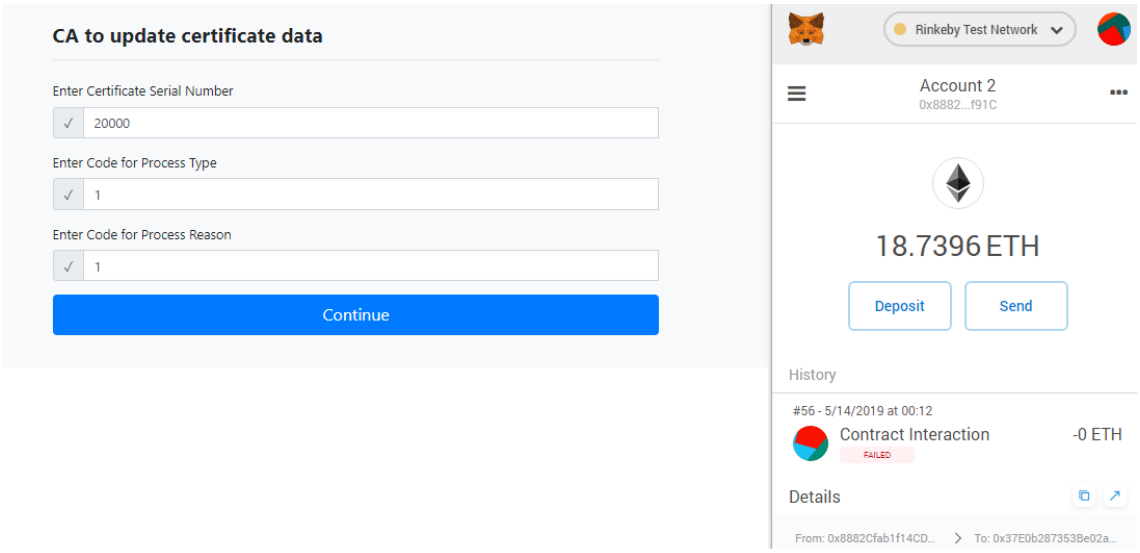
Bu çalışmada kullanıcılar için sertifikaların güncel ve geriye dönük durum bilgilerine kolay bir şekilde erişim imkanı sunulmuştur. Bu sorgulama yöntemi ayrıca adli işlemler gibi yüksek güvenilirliğe ihtiyaç duyulan durumlarda da verimlilik sağlayabilir. Blockchain ile ilgili varlıklar tarafından sürekli güncel, güvenilir ve kullanıcıya kullanım kolaylığı sağlayan bir yapı üzerinden başka bir üçüncü kişiye ihtiyaç olmadan daha hızlı sorgulamaların gerçekleştirilebilmesi sağlanmıştır. Çalışma için geliştirilen prototip dağıtık uygulamanın web tabanlı kullanıcı önyüzü sayesinde akıllı sözleşmede

programlanan iş akışlarının doğru kurgulandığı test edilmiştir. Şekil 8.1.'de akıllı sözleşmede yetkisi tanımlanan bir SM'ye ait kullanıcı sertifikası yayınlama testi gerçekleştirilmiştir. Yapılan test ile sadece akıllı sözleşmede yetki tanımlaması yapılan SM'lerin blockchaine veri yazabildiği doğrulanmıştır.



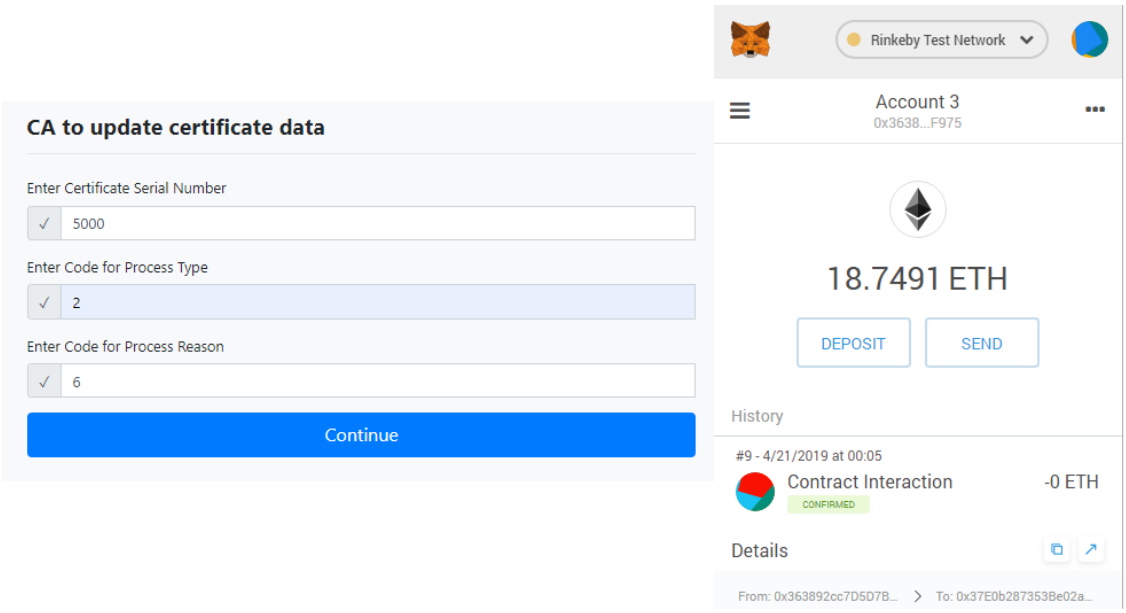
Şekil 8.1. Yetkili SM'nin kullanıcı sertifikası yayınlaması testi başarılı olmuştur.

Akıllı sözleşmede tanımlanan iş akışına göre SM'ler sadece kendi yayınladıkları sertifikalar için sertifika durum güncelleme işlemi yapabilir, diğer SM'lerin yayınladıkları sertifikalar sertifika durum bilgisi değişikliği yapamazlar. Örneğin olumsuz bir test senaryosu olarak SM ID numarası 3 olan alt SM tarafından yayınlanan sertifika, SM ID numarası 2 olan alt SM tarafından anahtar çalınma işlem nedeni ile iptal edilmek istenmiştir. Fakat SM ID numarası 2 olan SM'nin yayınladığı sertifikalarda güncelleme yapmak istediği sertifika seri numarası ile uyuşan bir sertifika olmadığından Şekil 8.2.'de görüldüğü gibi hata alınarak blockchain ağında işlemin yapılması engellenmiştir.



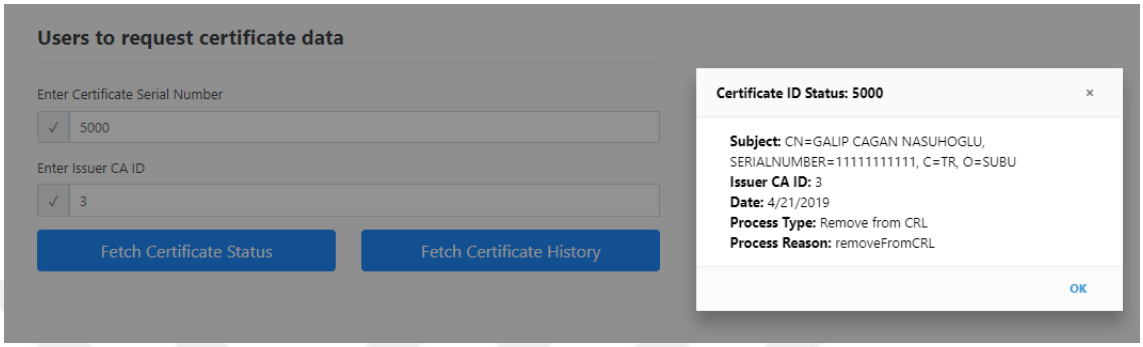
Şekil 8.2. Farklı bir SM tarafından yayınlanan sertifikanın durum değişikliği testi başarısız olmuştur.

Bir sertifikanın durum değişikliği sadece yayınlayan SM tarafından gerçekleştirilebilir. Örneğin SM ID'si 3 olan alt SM tarafından yayınlanan sertifikaya, aynı SM tarafından askıya alma testi uygulanmıştır. Şekil 8.3.'de görüldüğü gibi işlem başarılı bir şekilde gerçekleşmiştir.



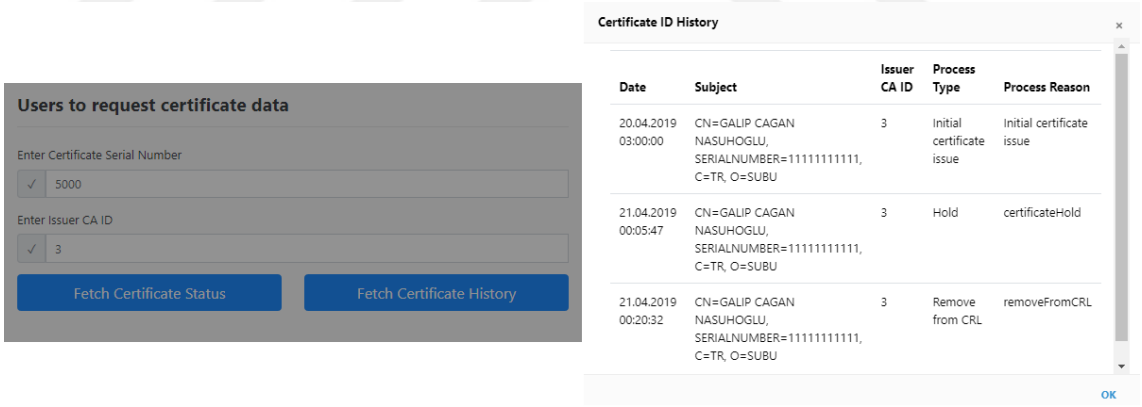
Şekil 8.3. Kendisini yayınlayan SM tarafından gerçekleştirilen sertifika durum değişikliği testi başarılı olmuştur.

Bir sertifikanın durumunu bütün kullanıcılar sorgulayabilmektedir. Örneğin bir sertifikaya askıdan indirme işlemi uygulanmış ve Şekil 8.4.'de görüldüğü gibi bir kullanıcı tarafından ilgili sertifikanın güncel durumu kontrol edilmiştir. Bir sertifikanın güncel durum veya sertifika tarihçesi, sertifika seri numarası ve yayınlayan SM ID bilgileri ile sorgulanabilmektedir.



Şekil 8.4. Bir sertifikanın güncel durum sorgulama sonucu

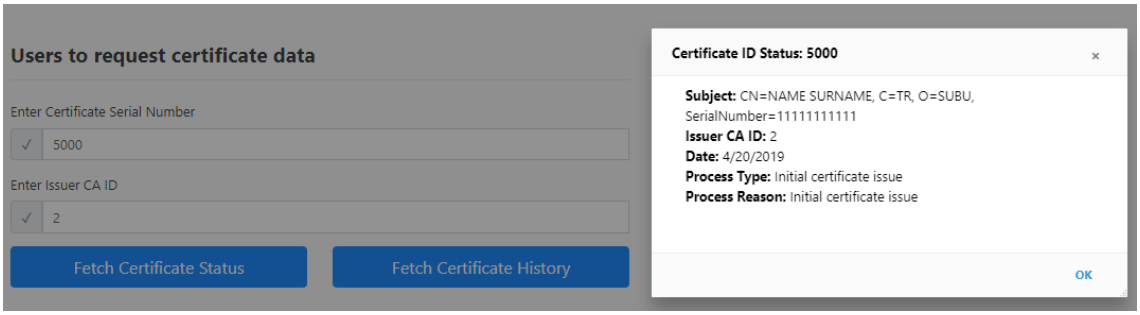
Bir sertifikanın geçmiş durum bilgilerine dair sertifika durum tarihçesi sorgulanabilir. Örneğin Şekil 8.5.'de bir sertifikanın durum tarihçesi sorgulaması yer almaktadır.



Şekil 8.5. Bir sertifikanın geriye dönük durum bilgileri

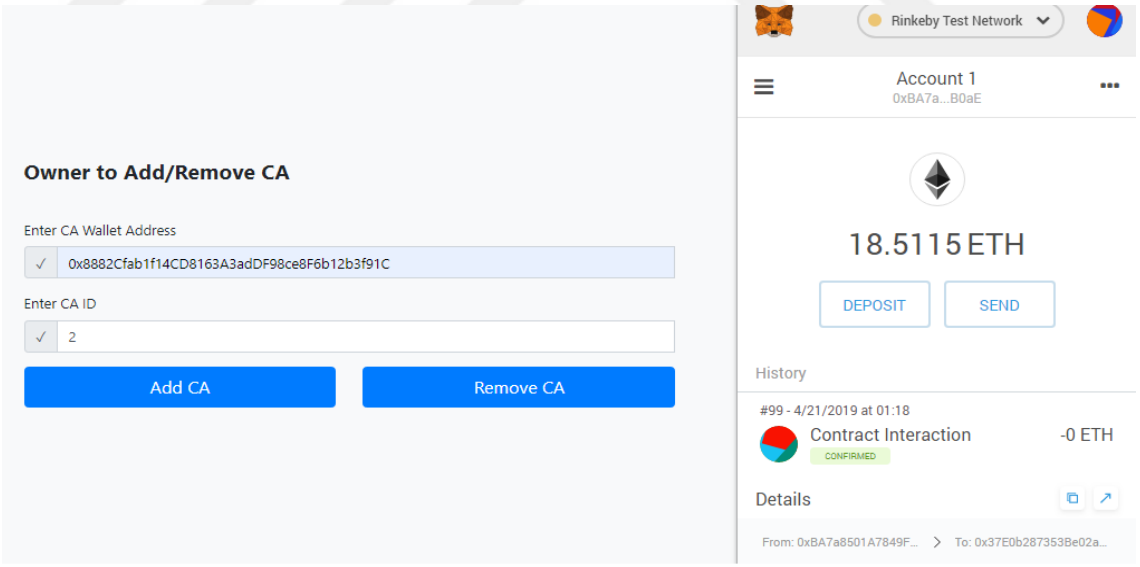
Farklı SM'lerin yayınladığı sertifikalar aynı sertifika seri numarasına sahip olabilirler. Aynı seri numarasına sahip sertifikalar, her SM'nin kendine özel bir ID'si olduğundan yayınlayan SM ID numarasıyla farklılaşarak ayırt edilebilirler. Özetle yayınlayan SM ID ve sertifika seri numarası değerleri tek bir sertifikayı işaret eder. Örneğin Şekil 8.6.'da görünen sertifika, SM ID'si 2 olan SM tarafından yayınlanmıştır. Aynı sertifika

seri numarası SM ID'si 3 olan SM tarafından da yayınlanmıştır. Bu durumda sorgulama yapılan SM ID'ye ait sertifika durum bilgisi blockchainden alınacaktır.



Şekil 8.6. Aynı seri numarasına sahip sertifikalar yayınlayan SM ID numarasıyla farklılaşarak ayırt edilebilirler.

Sistemde sorunlu bir alt SM fark edilirse, sertifika durum bilgisi yayınlaması için yetkisi alınarak sistemden izole edilebilir. Böyle bir durumda ilgili SM'nin geçmişte yayınladığı sertifika durum işlemlerine ait bilgiler ağdaki diğer dağıtık defterlerde muhafaza edilmeye devam edilmektedir. Örneğin Şekil 8.7.'deki gibi SM ID'si 2 olan alt SM'nin yetkisi sözleşme sahibi tarafından alınmıştır. Bu işlem sonucunda önceden yayınladığı sertifikalara ait durum bilgilerine ulaşılmaya devam edilmiştir.



Şekil 8.7. Bir alt SM'nin blockchaine yazma yetkisinin alınması

Blockchain teknolojisinin sağladığı yüksek veri bütünlüğü özelliği sayesinde geriye dönük olarak sertifika durum bilgilerinde değişiklik yapılamaz. Sertifika durum

bilgilerinin blockchain dağıtık defterlerinde tutulmasıyla geçmişe yönelik manipülasyonların önüne geçilmiştir ve güvenilir bir yapı sağlanmıştır.

8.2. Limitasyonlar

Yeni bir teknoloji olarak gelişimi ve değişimi devam eden bu yeni teknoloji, pilot uygulamalarla derin bir anlam kazanılması amacıyla araştırılmaya ve alınan başarılı sonuçlar sonrasında farklı alanlarda canlı sistemlere entegre edilmeye devam edilmektedir.

Bu çalışma kapsamında sertifika iptal bilgileri için dağıtık uygulama (DApp) tasarlanmıştır. Dağıtık uygulama, bir kullanıcı ön yüzü ve ethereum Rinkeby blockchain test ağı üzerinde çalışan akıllı sözleşmenin oluşturduğu bir arka yüzden oluşmaktadır. SM'lerin oluşturduğu blockchain ağ yönetimi ve SM Kayıt Servisi bu prototip uygulamanın kapsamı dışındadır. SM sertifikasının bir servis ile kaydedilmesi Google'ın Sertifika Şeffaflığı projesinde SSL sertifikaları için yapılan kayıt işlemine benzetilebilir. Mevcutta benzer bir sistem olduğundan SM Kayıt servisi üzerine yoğunlaşılmamış ve genel sistemin bir parçası olarak çalışmadaki görev tanımı yapılmıştır. Ethereum test ağları, işlemler için gerçek paralar kullanılmadan geliştirmecilerin kodlarını ve uygulamalarını test etmelerine imkan sağlar. Ethereum ana ağı ve test ağları arasındaki tek fark, farklı ağlarda yönetiliyor olmalarıdır. Kısıtlı zaman içerisinde tasarlanarak devreye alınan bu prototip dağıtık uygulama, akışlarının istenilen şekilde çalıştığının görülmesi açısından önemli olmuştur.

8.3. Gelecek Çalışmalar

Bu çalışma kapsamında yapılan blockchain dağıtık uygulaması test ağında gerçekleştirilmiştir. Rinkeby test ağının kullandığı PoA algoritması ile ethereum konsorsiyum veya özel ağda SM'lerin yetkili ağ düğümü olduğu bir yapı ileride daha kapsamlı bir çalışma olarak gerçekleştirilebilir. Canlı ortamda SM'ler arası yönetişim planlaması için konsorsiyum veya özel bir blockchain ağı kullanılması veri güvenliği ve gizliliği açısından çoğu kurumsal blockchain çözümünde olduğu gibi tercih edilen bir yöntemdir. Bu anlamda aynı ülkede veya farklı ülkelerdeki ESHS'ler arasında ortak bir konsensüs mekanizmasının olduğu bir konsorsiyum blockchain ağı kurulabilir. Böyle

bir dağıtık yapı ile merkezi yapıdan daha güvenilir, yüksek kayıt bütünlüğünün sağlandığı ve yüksek erişilebilirlik özelliğine sahip bir yapı hayata geçirilebilir.

Hızla dijitalleşmenin devam ettiği günümüzde blockchain teknolojisi kullanılarak sağlık, finans, lojistik gibi birbirinden farklı sektörlerde hizmet veren çalışmalar yapılabilmektedir. Özellikle sağlık sektörü geleneksel sistemlere dayanan ve değişim ihtiyacı duyan bir sektördür. Hastalara ait verilerin güvenli depolanması ve paylaşılması gibi önemli konular hastanelerin karşılaştığı zorluklardan birisidir. Güvenlik gerektiren verilerin güvenli bir şekilde saklanması ve yetkilere göre paylaşılması, blockchain teknolojisinin kullanılabileceği bir alandır.

KAYNAKLAR

Account Types, Gas, and Transactions. (2019). Erişim adresi: http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html

Akleylek, S., Yıldırım, H. M. ve Tok, Z. Y. (2011). Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta. *Akademik Bilişim 2011*, 713–718.

Ali, M. (2017). *Trust-to-Trust Design of a New Internet* (Doktora Tezi, Princeton University). Erişim adresi: https://muneebali.com/thesis

Antonopoulos, A. M. (2014). *Mastering Bitcoin*.

Aslan, F. Y. (2012). *Blok Şifrelerde Kullanılan Doğrusal Dönüşüm Yapılarının İncelenmesi*. (Yüksek Lisans Tezi, Trakya Üniversitesi) Erişim adresi: http://dspace.trakya.edu.tr/xmlui/bitstream/handle/1/1443/49.pdf?sequence=1.

Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D. ve Spalazzi, L. (2017). *Certificate Validation through Public Ledgers and Blockchains*. *First Italian Conference on Cybersecurity (ITASEC17)*, 557–564.

Başçi, G. Ç. (2008). Sertifika Geçerlilik Kontrolündeki Sorunlarin Giderilmesi. *TÜBİTAK Kamu Sertifikasyon Merkezi*, 6. Erişim adresi: http://www.kamusm.gov.tr/dosyalar/makaleler/Sertifika Gecerlilik Kontrolundeki Sorunlarin Giderilmesi.pdf

Bawa, M., Cooper, B. F., Crespo, A., Daswani, N., Ganesan, P., Garcia-Molina, H., … Yang, B. (2003). Peer-to-peer Research at Stanford. *SIGMOD Rec.*, *32*(3), 23–28. Erişim adresi: https://doi.org/10.1145/945721.945728

Bitcoin Hashrate Distribution. (2019, 23 Mart). Erişim adresi: https://www.blockchain.com/pools

Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S. ve Cooper, D. (2008, Mayıs). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280)*. https://doi.org/10.17487/RFC5280

Bozic, N., Pujolle, G. ve Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. *3rd Smart Cloud Networks & Systems (SCNS)*, 1–8. Erişim adresi: https://doi.org/10.1109/SCNS.2016.7870552

Bralić, V., Kuleš, M. ve Stančić, H. (2017). A Model for Long-term Preservation of Digital Signature Validity: TrustChain. Erişim adresi: https://doi.org/10.17234/INFUTURE.2017.10

Carlsson, B. ve Gustavsson, R. (2001). The Rise and Fall of Napster - An Evolutionary Approach. *Active Media Technology* (ss. 347–354). Springer Berlin Heidelberg.

Çelik, V. ve Adalier, O. (t.y.). *Türkiye Cumhuriyeti Kimlik Kartı (TCKK) ve Elektronik İmza*. Erişim adresi: http://www.kamusm.gov.tr/dosyalar/bildiriler/Turkiye_Cumhuriyeti_Kimlik_Karti_ve_Elektronik_Imza.pdf

Chen, J., Yao, S., Yuan, Q., He, K., Ji, S. ve Du, R. (2018). CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2060-2068.

Comodo Security Solutions. (2011, 31 Mart). *Comodo Fraud Incident*. Erişim adresi: https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Courtois, N. ve Bahack, L. (2014). *On subversive miner strategies and block withholding attack in bitcoin digital currency*.

Digibyte. (2018, 10 Nisan). European countries join Blockchain Partnership. Erişim adresi: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

Eckersley, P. (2011, 5 Mayıs). A Syrian Man-In-The-Middle Attack against Facebook. Erişim adresi: https://www.eff.org/tr/deeplinks/2011/05/syrian-man-middle-against-facebook

Erzincan, Ö. D. (2004). E-imza Deneyimi. *Telekom Dünyası Dergisi.*, s. 32.

Eyal, I. ve Sirer, E. (2013). *Majority Is Not Enough: Bitcoin Mining Is Vulnerable* (C. 8437). Erişim adresi: https://doi.org/10.1007/978-3-662-45472-5_28

Global Sign. (2011). *Security Incident Report*. Erişim adresi: https://www.globalsign.com/en/resources/globalsign-security-incident-report.pdf

Hasircioğlu, I. ve Öz, D. (2008). *Yapilandirilabilir Ve Dinamik Bir Sertifika Doğrulama Kütüphanesi Modeli*. Erişim adresi: http://www.emo.org.tr/ekler/a44180ab9ab950e_ek.pdf

Herranz, J. (2007). Identity-based ring signatures from RSA. *Theoretical Computer Science*, 100–117.

International Telecommunication Union. (1997). *ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Authentication framework*.

Karaaslan, E. ve Akbas, M. F. (2017). Blokzinciri Tabanli Siber Güvenlik Sistemleri. *Uluslararasi Bilgi Güvenliği Mühendisliği Dergisi*, *3*(2), 16–21. Erişim adresi: https://doi.org/10.18640/ubgmd.373297

Kardaş, S. (2018). Blokzincir Teknolojisinde Uzlaşma Modelleri. *1. Ulusal Blokzincir Çalıştayı*.

Kaya, K. (2018). *Blok Zinciri "Kriptonun Doğuşu"*. Kemal Kaya.

Kehrli, J. (2016, 7 Ekim). Blockchain explained. Erişim Adresi: https://www.niceideas.ch/roller2/badtrash/entry/blockchain-explained-beta

Kırbaş, İ. (2018). Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları. *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 75–82. Erişim adresi: https://doi.org/10.29048/makufebed.365066

Kırımlı, M. ve Erdem, A. (t.y.). *Açik Anahtar Kriptografisi İle Sayisal İmza Tasarimi Ve Uygulamasi*.

Laurie, B., Langley, A. ve Kasper, E. (2013). *Certificate Transparency (RFC 6962)*. Erişim adresi: https://tools.ietf.org/html/rfc6962

Malone, D. ve O'Dwyer, K. J. (2014). *Bitcoin Mining and its Energy Footprint*. Erişim adresi: https://doi.org/10.1049/cp.2014.0699

Meijer, D. B. (2017). *Consequences of the implementation of blockchain technology* (Yüksek Lisans Tezi, Delft University of Technology). Erişim adresi: http://resolver.tudelft.nl/uuid:da0b8d80-d19e-4149-bfbd-64b0ca79042a

Mendi, A. F. ve Çabuk, A. (2018). Bitcoin'in Arkasindaki Güç: Blockchain. *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, *1*(1), 12–23.

Montresor, A. (2008). Decentralized Network Analysis: A Proposal. *2008 IEEE 17th*

Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 111–114. Erişim adresi: https://doi.org/10.1109/WETICE.2008.36

Morton, B. (2013, 4 Ocak). TURKTRUST Unauthorized CA Certificates. Erişim adresi: https://www.entrustdatacard.com/blog/2013/january/turktrust-unauthorized-ca-certificates

Murat, M. (2018). *Blockchain and secure electronic healthcare system*. (Yüksek Lisans Tezi, İstanbul Technical University), YÖK.

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system*. 9.

Nath, A., Ghosh, S. ve Alam Mallick, M. (2010). Symmetric Key Cryptography Using Random Key Generator. *International Conference on Security & Management*. Las Vegas Nevada.

Öğretmen, B. (t.y.). Çevrimiçi Sertifika Durum Protokolü (OCSP). Erişim adresi: https://www.researchgate.net/publication/266586961_CEVRIMICI_SERTIFIKA_DURUM_PROTOKOLU_OCSP

Resmi Gazete. (2004). *5070 Elektronik İmza Kanunu*. Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm

Resmi Gazete. (2005). Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik. Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2005/01/20050106-15.htm

Rinkeby: Ethereum Testnet. (2019, 8 Ocak). Erişim adresi: https://www.rinkeby.io/#stats

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S. ve Adams, D. C. (2013). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC6960)*. Erişim adresi: https://doi.org/10.17487/RFC6960

Santesson, S., Polk, T. ve Nystrom, M. (2004). *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (RFC3739)*. Erişim adresi: https://tools.ietf.org/html/rfc3739

Shafa'amry, M., ve Alam Aldeen, N. (2009). Activate the Dynamic Delegation Process in X.509 Certification via a new Extension. WSEAS TRANSACTIONS on COMPUTERS, ISSN: 1109-2750, 8, 355–364.

Soghoian, C. ve Stamm, S. (2011). *Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*.

Taş, O. ve Kiani, F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme. *Bilişim Teknolojileri Dergisi*, *11*(4), 369–382. Erişim adresi: https://doi.org/10.17671/gazibtd.451695

Thakur, J. ve Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, *1*(1), 7.

TUBITAK Kamu Sertifikasyon Merkezi. (2018). *Nitelikli Elektronik Sertifika Uygulama Esasları*. (12), 67.

Ünsal, E. ve Kocaoğlu, Ö. (2018). Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. *European Journal of Science and Technology*, 54–64. Erişim adresi: https://doi.org/10.31590/ejosat.423676

Usta, A. ve Doğantekin, S. (2017). *Blockchain 101*. Erişim adresi: https://docplayer.biz.tr/108651670-Blockcha-n-101-ahmet-usta-serkan-dogantekin.html

Wood, G. (2014). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. Erişim adresi: https://pdfs.semanticscholar.org/ee5f/d86e5210b2b59f932a131fda164f030f915e.pdf?_ga=2.165412927.1669833658.1556011654-2083167559.1555092951

Yakubov, A., Shbair, W. M., Wallbom, A., Sanda, D. ve State, R. (2018). A blockchain-based PKI management framework. *In The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS*, 1–6.
Erişim adresi: https://doi.org/10.1109/NOMS.2018.8406325

Yalçınkaya, B. (2008). *Elektronik İmzali Belgelerin Yönetimi Ve Arşivlenmesi*. (Yüksek Lisans Tezi, Marmara Üniversitesi) Erişim adresi: http://bbytezarsivi.hacettepe.edu.tr/jspui/bitstream/2062/253/1/161.pdf.

Yıldırım, F. (2015). Blok Zinciri Teknolojisi ve Uluslararası İlişkilere Muhtemel Etkileri. *Medeniyet Araştırmaları Dergisi*, *2*(4), 81–97.

Yılmaz, M. (2016). Elektronik İmzali Belgelerin Karşilaştirmali Hukukta ve İdarî Yargilama Hukukunda Delil Niteliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, *22*(3), 3435–3486.

Yu, J. ve Ryan, M. (2017). Evaluating Web PKI. *In Software Architecture for Big Data*

and the Cloud, 105–126.

Yüksel, M. (2018, 6 Haziran). Sertifika Şeffaflığı. Erişim adresi: http://www.cezerisga.com/makale/sertifika-seffafligi

Zhang, A. ve Ma, X. (2018). Decentralized Digital Certificate Revocation System Based on Blockchain. *Journal of Physics: Conference Series*, *1069*, 12125. Erişim adresi: https://doi.org/10.1088/1742-6596/1069/1/012125

Zheng, Z., Xie, S., Dai, H., Chen, X. ve Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *In 2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. Erişim adresi: https://doi.org/10.1109/BigDataCongress.2017.85

Zusman, M. (2008). *Criminal charges are not pursued: Hacking PKI*. Erişim adresi: https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-zusman-hacking_pki.pdf

ÖZGEÇMİŞ

Galip Çağan Nasuhoğlu, 13/11/1987'da Sivas'ta doğdu. İlk, orta ve lise eğitimini Sivas'ta tamamladı. 2005 yılında başladığı Uluslararası Kıbrıs Üniversitesi Elektrik - Elektronik Mühendisliği Bölümü'nü 2010 yılında bitirdi. 2011 yılında Sakarya Üniversitesi Elektrik - Elektronik Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı. Yüksek lisans derslerini tamamlamanın ardından sırasıyla AstraZeneca, Vodafone Türkiye, TEB firmalarında çalıştı. 15/01/2018 tarihinden itibaren TÜBİTAK Bilgem'de kariyerine devam etmektedir.