Türkiye Standartlarına Uygun Blokzincir Tabanlı Diploma Yönetimi

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Ekrem Yasir İKIZOĞLU

tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül .....
(Tez Danışmanı)

Dr. Oktay Adalıer .....
(Tez Eş-danışmanı)

Prof. Dr. Selim Zaim .....

Prof. Dr. Nizamettin Bayyurt .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 30.07.2019

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Ekrem Yasir İKIZOĞLU, başlığı, 'Türkiye Standartlarına Uygun Blokzincir Tabanlı Diploma Yönetimi' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 

Tarih: 30.07.2019

Blockchain Based Diploma Management In Turkey Standards

Ekrem Yasir İKIZOĞLU

Abstract

Organization's stamp or wet signature are used to approve and confirm the validity of important documents such as certificate and diploma. However, in today's technology, it is quite easy to imitate stamps and signatures, produce documents like the original and very difficult to understand the fake ones. Because of such fraud many private and public institutions are employing unqualified and unreliable employees. It is very difficult to verify institutions which issued these documents. In this study, the scope of the creation and validation of valuable documents was defined by using blockchain technology. Also, examples in the World and the degree (diploma) management dimension in Turkey were discussed. Data structures in accordance with the standards and applied regulations in our country have been examined and requirements were determined. Blockcerts solution working on blockchain architecture has been chosen according to the requirements. Classical methods for diploma verification in Turkey were also compared with equivalents in the World. Finally, a proved architecture was adapted as an alternative to Turkey's diploma verification structure.

Keywords: Blockchain, Education, Diploma, Validation, Decentralized

Türkiye Standartlarına Uygun Blokzincir Tabanlı Diploma Yönetimi

Ekrem Yasir İkizoğlu

Öz

Diploma, sertifika gibi önemli belgeler kuruluş kaşesi veya ıslak imza ile onaylanmakta, geçerliliği doğrulanmaktadır. Fakat günümüz teknolojisinde kaşe ve imzaların taklit edilmesi, belgenin orijinali gibi üretilmesi oldukça kolay ve sahtesinin anlaşılması da bir o kadar zordur. Birçok kamu ve özel kuruluş bu tarz sahtecilik girişimleri sebebiyle kalifiyesiz, güvenilmez eleman çalıştırmaktadır. Değeri yüksek belgeleri veren kurumların doğrulanmasının yapılması zordur. Bu çalışmada değerli belgelerin oluşturulması ve doğrulaması işlemlerinin tanımı yapılarak bunun blokzincir teknoloji ile gerçekleştirilmesi tanımlanmıştır. Ayrıca dünyadaki örnekleri ve Türkiye'de ki diploma yönetimi boyutu ele alınmıştır. Ülkemizdeki uygulanan yönetmeliklere, standartlara uygun veri yapıları araştırılmış ve ihtiyaçlar belirlenmiştir. Belirlenen ihtiyaçlar doğrultusunda blokzincir mimarisi üzerinde çalışan Blockcerts çözümü seçilmiştir. Yapılan çalışma Türkiye'deki klasik çözüm metodu ve dünyadaki yapılan muadilleri ile karşılaştırılmıştır. Dünyada kabul görmüş Blockcerts mimarisini kullanarak Türkiye'de kullanılan diploma doğrulama yöntemine bir alternatif metot geliştirilmiştir.

Anahtar Sözcükler: Blokzincir, Eğitim, Diploma, Doğrulama, Merkezsiz

Teşekkür

Çalışmalarım boyunca maddi manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme ve kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösterici ve destek olan değerli Prof. Dr. Ensar Gül ile Dr. Oktay Adalıer danışman hocamlarıma sonsuz teşekkürler ederim...

İçindekiler

Abstract iii

Öz iv

Teşekkür v

Şekil Listesi viii

Tablo Listesi ix

Kısaltmalar x

1 Giriş 1

2 İlişkili Çalışmalar 3
2.1 Diploma Gereklilikleri . . . 3
2.2 Uyum Standartları . . . 4
2.3 Diploma Doğrulama Çözümleri . . . 7
2.3.1 Geleneksel Çözümler . . . 7
2.3.2 Dijital Merkezi Çözümler . . . 7
2.3.3 Dijital Merkezsiz Çözümler . . . 10
2.4 Metotların Karşılaştırılması . . . 13

3 Blokzincir 15
3.1 Blokzincir Tarihi . . . 15
3.2 Blokzincir Mimarisi . . . 15
3.2.1 Konsensus Katmanı . . . 16
3.2.2 Madencilik Katmanı . . . 17
3.2.3 Dağılım ve Transfer Katmanı . . . 18
3.2.4 Doğrulama Katmanı . . . 19
3.2.5 Uygulama Katmanı . . . 20
3.3 Blokzinciri Önemli Yapan Özellikler . . . 22
3.4 Kayıt Edilebilen Data Türleri . . . 23
3.5 Blokzincir Ağ Türleri . . . 24
3.5.1 İzinsiz Açık Blokzincir . . . 24
3.5.2 İzinsiz Gizli Blokzincir . . . 24
3.5.3 İzinli Açık Blokzincir . . . 24
3.5.4 İzinli Gizli Blokzincir . . . 25

4 Blockcerts **26**
4.1 Dijital Diploma Oluşturma . . . 26
4.2 Dijital Diploma İmzalama ve Yayınlama . . . 27
4.3 Dijital Diploma Paylaşımı . . . 29
4.4 Dijital Diploma Doğrulama . . . 30

5 Türkiye'de Diploma **32**
5.1 Kullanımdaki Diploma Alanlarının Çıkartılması . . . 32
5.2 Diploma Eki . . . 33

6 Türkiye'de Blokzincir Tabanlı Diploma Yönetimi **34**
6.1 Gereksinim Analizi . . . 35
6.2 Süreç Analizi . . . 36
6.3 Talep Toplama ve Diploma Oluşturma . . . 37
6.4 Diploma Yayınlama Tasarımı . . . 38
6.5 Paylaşım Süreç Tasarımı . . . 39
6.6 Doğrulama Süreç Tasarımı . . . 39
6.7 Diploma Tasarımı . . . 40
6.8 Entegrasyon Efor Analizi . . . 42

7 Sonuç **43**

Kaynaklar **45**

Şekil Listesi

2.1 Hologram 7
2.2 Sakarya Üniversitesi Diploma Doğrulama Sistemi 8
2.3 Üniversitelerin Diploma Doğrulama Mimarisi 8
2.4 E-Devlet Diploma Doğrulama Mimarisi 9
2.5 Merkezsiz Blokzincir Tabanlı Çözüm Mimarisi 10
2.6 Blockcert Akış Şeması 12

3.1 Blokzincir Tabanlı Uygulamaların Katmanları 16
3.2 X-Hashcash SMTP Başlık İçerik Örneği 17
3.3 Ana ve Yetim Zincir Gösterimi 18
3.4 Merkle Root Hesaplama Şeması 20
3.5 Bitcoin Bloklarınn Bağ Gösterimi [1] 22
3.6 Bitcoin İmzalama ve Doğrulama İşlemleri [1] 23

4.1 Diploma Özeti İçeren İşlem Detayları 29
4.2 Blockcerts Doğrulama Adımları 31

6.1 Süreçler 36
6.2 Dijital Diploma Oluşturma Şeması 37
6.3 Dijital Diploma Yayınlama Şeması 38
6.4 Dijital Diploma Paylaşım Şeması 39
6.5 Dijital Diploma Doğrulama Şeması 40
6.6 Blokzincir Üzerinde Yayınlanmış Diploma Örneği 41

Tablo Listesi

2.1 IMS Global Learning Consortium Örnek JSON-LD 6
2.2 Farklı Çözümlerin Karşılaştırılması 13

3.1 Bitcoin Blok Başlıklarının Örnek Gösterimi 19
3.2 Bitcoin İşlem Yapısı 21

4.1 İmzalanmamış Dijital Diploma 27
4.2 İmzalanmış Diplomanın Ek Alan İçeriği 28

5.1 Diploma Alanlarının Kullanım Oranı 32

6.1 Talep Toplama Yalancı Kod 38
6.2 Dijital Diploma Oluşturma Yalancı Kod 38
6.3 Yayınlama Yalancı Kod 38
6.4 Paylaşım Yalancı Kod 39
6.5 Kullanılan Ürünlerin Gelişme Maliyet Tablosu 42

Kısaltmalar

BTC	Bitcoin
ETH	Etherium
REST	Representational State Transfer
API	Application Programming Interface
JSON	JavaScript Object Notation
JSON-LD	JSON for Linking Data
ECDSA	Elliptic Curve Digital Signature Algorithm
SHA	Secure Hash Algorithm
YÖK	Yüksek Öğretim Kurumu
UNESCO	United Nations Educational, Scientific and Cultural Organization
CEPES	European Centre for Higher Education
IMS	Instructional Management Systems
POW	Proof of Work
HTML	Hypertext Markup Language
SNHU	Southern New Hampshire University

Bölüm 1

Giriş

İş, meslek veya sanat sahibi olabilmek, kariyer edinebilmek için birçok eğitimler alınarak bireyler yeterliliklerini arttırmaktadır. Yeterlilikleri arttırmanın yanında bu becerileri temin ettiklerine, eğitimi başarıyla tamamladıklarına dair diploma ve sertifikalara delil olarak ihtiyaç duyulmaktadır. Okul, üniversite gibi eğitim kurumlarının yanında özel firmalar kendi formatlarında ya da bağlı oldukları kanun ve yönetmeliklere göre diploma ve sertifikaları kağıt baskı olarak veya dijital ortamda üretip bireylere iletmektedirler. Diploma üzerine kaşe, damga gibi güvenlik gerekçesi ile önlemler alınsa da yetkinliği olmayan bireyler hedeflerine ulaşmak için diploma gibi değerli dokümanları belli platformlar üzerinden kolaylıkla temin edebilmektedir [2]. Yakın tarihimizde üniversitelerde, özel kurumlarda ve ülke için kritik pozisyonda bulunan firmalarda sahte diploma vakaları meydana gelmiştir [3, 4]. Dünyada da belge sahteciliği üzerine birçok çalışma bulunmaktadır. Çalışmalarda sahte diploma temininin ve problemin boyutları ortaya konulmaktadır [5]. Belge doğrulamasının pahalı, yavaş ve yeterli güvenlik seviyesinde olmamasından dolayı işe alım süreçlerinde, maaşın belirlenmesinde veya terfi durumlarında yanlış uygulamaların meydana gelmesine yol açmaktadır. Doğrulama mekanizmasının yetersiz kalması veya yavaş işlemesinden dolayı meydana gelen bu vahim olaylar neticesinde kurumlar zarar görmekte hatta kritik makamlarda yeterliliği olmayan kişiler görev almaktadır [6]. Doğrulama sürecinin zaman, para ve insan gücü maliyetinin az olması yanı sıra güven sağlayan yöntemleri içermesi gerekmektedir. Diplomayı veren kuruluşun doğrulanması, yeterliliği olan kişinin kimliği ve bunun yanında kişinin ne gibi yetkinliğe sahip olduğunun doğrulanması gerekmektedir. Bu probleme istinaden Türkiye'de e-devlet platformu üzerinden yükseköğretim mezun belgesi sorgulama, doğrulama hizmeti

geliştirilmiştir [7]. Fakat geleneksel merkezi veri tabanları üzerine kurulan bunun gibi yapılar mevcut verinin değiştirilmesi, bozulması veya erişimin kesilmesi gibi problemler barındırmaktadır [8]. Bu sebepten daha güvenilir, hızlı ve kolay doğrulama yapılabilecek bir çözüm ihtiyacı bulunmaktadır..

Dünyada diploma, sertifika gibi değerli dokümanların hızlı, güvenilir bir yöntemle doğrulanması için blokzincir tabanlı çözümler geliştirilmiştir [9–11]. Fakat geliştirilen bu çözümlerin Türkiye standartlarına uyumluluğu sorun oluşturmaktadır. Mevcut çözümlerin Türkiye üniversitelerinde de kullanımının sağlanması için bazı ek standartların belirlenmesi gerekmektedir. Çalışmamızda blokzincir yapısının güvenilirliğinin yanında diploma doğrulama sürecindeki mevcut problemleri giderebilme yeteneği incelenmiştir. Türkiye'de bulunan çözümler ile uluslararası çözümlerin karşılaştırılması yapılmıştır. Türkiye'deki üniversitelerde diploma oluşturulmasında uygulanan standartlar ile Blockcerts sertifika yapısının ilişkilendirilmesi yapılmış, ihtiyaçların tespiti sonrası gerekli ek çözümler sunulmuştur [12]. Dünyaca kabul görmüş bir yapı ile Türkiye'nin standartlarına uygun diploma doğrulama yapısını uluslararası bir konuma taşıma çalışması gerçekleştirilmiştir. Bu çalışma örnek olması açısından T.C. İstanbul Şehir Üniversitesi Öğrenci İşlerinde diploma süreçlerinde uygulanarak klasik kağıt bazlı diplomanın yanında öğrencilere blokzincirde doğrulaması mümkün olan dijital diploma üretim çalışması yapılmıştır.

Bölüm 2

İlişkili Çalışmalar

Bu bölümde diplomada olması gereken fonksiyon gereklilikleri incelenmiş olup, kullanımda olan yönetmelikler detaylandırılmıştır. Dünyada doğrulama süreci için geliştirilmiş mevcut çözümler araştırılmış ve geleneksel, dijital merkezli ve dijital merkezsiz şeklinde gruplandırılarak bahsedilmektedir. Mevcut çözümlerin ele alınması sonrasında Türkiye'nin mevcut yapısı ile diğer metotların güvenlik, hız, iptal edilebilirlik, uyumluluk, kalıcılık ve merkezsizlik kapsamında karşılaştırılması yapılmıştır.

2.1 Diploma Gereklilikleri

Bir okul veya öğrenim programının başarıyla tamamlandığını, kazanılan yetkinliği gösteren diplomalar belli başlı karakteristiği bünyesinde barındırmalıdır.

- Bilgilendirici; Sağlanan başarının ne ifade ettiği, hangi konuda başarı sağlandığı gibi gerekli bilgileri içermelidir. Diplomayı kontrol eden kişinin bu veriler ile kişinin yeteneğini, başarısını veya kazanmış olduğu yetkinliği anlayabilmelidir.
- İptal Edilebilir; Verilen diplomalar belli bir nedenden dolayı verilen kurum tarafından iptal edilebilmelidir. Böylelikle bir sebepten dolayı geçerliliğini yitiren diplomaların bu fonksiyon ile kullanım dışı tutulması sağlanmalıdır.
- Paylaşılabilir; Diplomayı almaya hak kazanan kişiler belgelerini dilediği gibi paylaşabilmelidir.

- Doğrulanabilir; Diplomaların doğrulanması herkesçe yapılabilmelidir. İşveren, eğitim kurumları veya kişiler diplomanın doğrulamasını kolaylıkla yapabilir olmalıdır. Diplomanın değişikliğe uğramadığını çözümlemek için kullanılan metodunda güvenilir, iyi tasarlanmış ve kolay uygulanabiliyor olması gerekmektedir.

- Veren-Alan; Diploma içerisinde diplomayı veren kurum, alan birey veya kurumların belirgin bir şekilde tanımlanıyor olması gerekmektedir. Doğrulama sırasında bu sahipliklerin kontrolleri yapılmalıdır.

- Standartlara uyumlu; Oluşturulan diplomalar bulunduğu ülkenin veya bağlı olduğu kurum ve kuruluşların yayınladıkları yönetmeliklerinin koyduğu standartlara uyumlu olmalıdır.

2.2 Uyum Standartları

Diploma oluşturma sırasında kullanılan niteliklerin farklı bölge ve kurumlar için anlaşılır formatta olması geçerlilik ve doğrulama işlemleri için önem arz etmektedir. Bir bölgede verilen diploma belgesinin bağlı olduğu ülke, kurum veya birlikteliklerin koymuş olduğu standartlara uyması ortak bir dil oluşması açısından gereklidir. Bu sebepten ülkeler kanunlar ve yönetmelikler ile bünyesinde barındırdığı kurumlar için bir yol haritası belirlemektedir.

Türkiye'deki lisans, yüksek lisans ve doktora gibi öğrenim programlarını yönetmek, düzenlemek ve denetlemek için Yükseköğretim Kurulu (YÖK) kurulmuştur. YÖK'e bağlı her üniversite YÖK tarafından yayınlanan yönetmelik ve mevzuatlara uymak zorundadır [13]. YÖK yönetmeliğinde diploma üzerinde alan kişinin kayıtlı olduğu enstitü anabilim/ana sanat dalındaki programın Yükseköğretim Kurulu tarafından onaylanmış adının bulunması gerektiği belirtilmiştir [14]. Yükseköğretim kanununda diplomalarla ilgili esasların üniversitelerce hazırlanmasını belirtmiştir. Buna istinaden Türkiye'deki üniversiteler eğitim-öğretim ve diploma yönetmeliklerinde uyguladıkları diploma standartlarını belirtmişlerdir. Sadece verildiği ülkede ne anlama geldiği bilinen diplomanın uluslararası, diğer ülkeler arasında da anlaşılır olması için diplomanın yanında diploma eki de yükseköğretim kurumlarınca verilmektedir [15–17]. Avrupa Komisyonu, Avrupa Konseyi ve UNESCO/CEPES tarafından belirlenen format ile Avrupa birliği tarafında kabul edilerek 22 ülke tarafından kullanılmaktadır [15]. Kazanılan başarının uluslararası yeterli düzeyde

tanınmasını sağlayan diploma eki Türkiye'de de diploma ile beraber verilmektedir [17]. Türkiye'deki üniversitelerin şeffaflığının artırılması, mezunların ulusal düzeyde iş bulma imkanının sağlanması ve tüm Avrupa'da kabul gören anlaşılır ortak dilde diploma oluşturma amacıyla diploma eki üretilmekte ve mezun bireylere Türkiye'deki her üniversite tarafından iletilmektedir.

Open Badge; Misyonu, eğitime katılım ve kazanımı uygun şekilde ölçeklendirebilecek ve geliştirebilecek teknolojiyi ilerletmek olan ve bu çerçevede etkili eğitim kurumları, tedarikçiler ve devlet kuruluşları ile birlikte standartlar geliştiren IMS Global Learning Consortium tarafından, dijital ortamda hangi yetkinliğin kim tarafından kime verildiğinin uygun bir formatta ifade edilmesi ve doğrulanması amacıyla geliştirilen bir standarttır [18]. JSON-LD veri yapısını kullanıldığı bu standartta alıcı, verici kimliklerinin yapı içerisindeki bağlantılar ile doğrulanması sağlanmaktadır. Kurum veya kuruluşlardan kazanılan yetenek, ödül veya yetkinlik gibi bireyin gelişimini gösteren dijital rozetlerin paylaşılması, gösterilmesi ve doğrulaması için bir standart sunmaktadır. Bu standart aynı zamanda blokzincir altyapısı üzerine inşa edilmiş olan Blockcerts çözümü içerisinde de kullanılmaktadır [19].

TABLO 2.1: IMS Global Learning Consortium Örnek JSON-LD

```
{
  "@context": "https://w3id.org/openbadges/v2",
  "id": "https://example.org/assertions/123",
  "type": "Assertion",
  "recipient": {
    "type": "email",
    "identity": "alice@example.org"
  },
  "issuedOn": "2016-12-31T23:59:59+00:00",
  "verification": {
    "type": "hosted"
  },
  "badge": {
    "type": "BadgeClass",
    "id": "https://example.org/badges/5",
    "name": "3-D Printmaster",
    "description": "This badge is awarded for passing...",
    "image": "https://example.org/badges/5/image",
    "criteria": {
      "narrative": "Students are tested on knowledge..."
    },
    "issuer": {
      "id": "https://example.org/issuer",
      "type": "Profile",
      "name": "Example Maker Society",
      "url": "https://example.org",
      "email": "contact@example.org",
      "verification": {
        "allowedOrigins": "example.org"
      }
    }
  }
}
```

TABLO 2.1. de IMS Global Learning Consortium tarafından belirlen JSON formatında örnek diploma veri yapısı görüldüğü üzere içerisinde yetkinlik, diplomanın amacı, veren makam gibi alanlar açık bir şekilde ifade edilmektedir.

2.3 Diploma Doğrulama Çözümleri

Diplomanın sahtesinin tespiti için günümüzde geleneksel çözümlerin yanı sıra dijital ortam çözümleri geliştirilmiştir. Bu bölümde ortaya konmuş olan çözümlerin incelemesi yapılmaktadır.

2.3.1 Geleneksel Çözümler

Günümüzde diplomalar kağıt baskı üzerinde verilmeye devam edilmektedir. Bu fiziki dokümanların taklidini önleyebilmek için her kurum kendi yönetmeliğinde yer alan çözümler ile önlemler almaktadır [20].

Şekil 2.1: Hologram

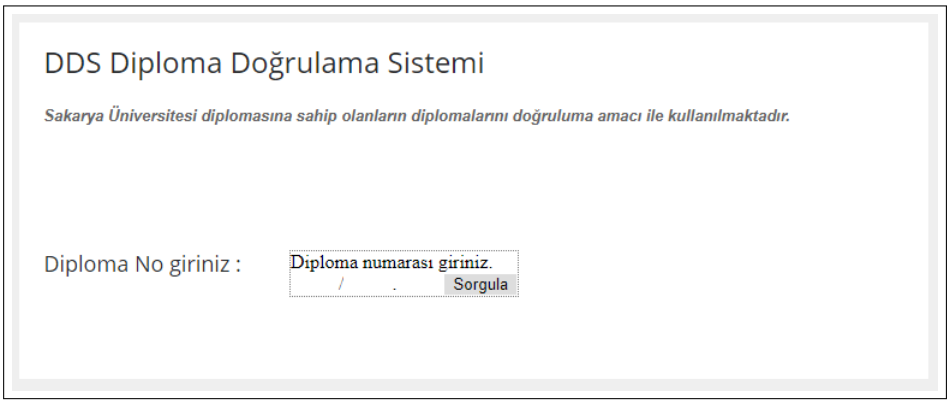
ŞEKİL 2.1 deki gibi hologram veya ıslak imza, özel tasarım şablonlar, kabartma gibi özel baskı metotları ile belgenin sahte olup olmadığının doğrulanması hedeflenmiştir. Fakat günümüz teknolojisinde kabartma, hologram veya ıslak imzalar kolayca taklit edilebilmektedir [2, 5, 21].

2.3.2 Dijital Merkezi Çözümler

Geleneksel kağıt üzerinden yapılan doğrulamalara ek olarak üniversiteler verdikleri belgelerin doğruluğunun yapılabilmesi için kendi web sayfalarına yönlendiren bağlantıları diploma üzerine işlemektedirler.

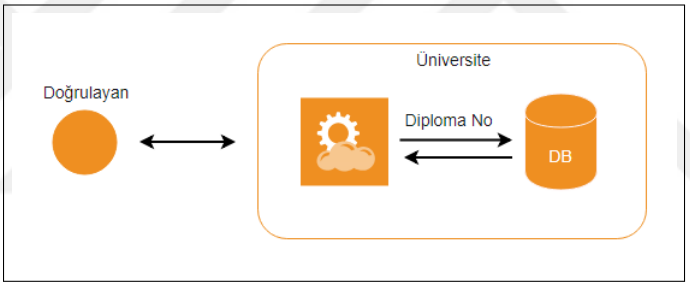
ŞEKİL 2.2 de görüleceği üzere bu sayfalarda belge numarası istenebilmekte veya yönlendirmeler ile kurum ile irtibata geçilmesi gerektiği belirtilmektedir. Kendi merkezi veri tabanları üzerinden yaptıkları sorgular ile doğrulamayı kısmen sağlamaktadırlar.

Oxford Üniversitesi işverenlere ücretli doğrulama servisi hizmeti vermektedir [22]. Cambridge Üniversitesi kendi sayfasındaki yönlendirmelerinde bulunan mail adresi üzerinden doğrulama süreci sunmaktadır [23]. Sakarya Üniversitesi'nde ise diploma üzerindeki



Şekil 2.2: Sakarya Üniversitesi Diploma Doğrulama Sistemi

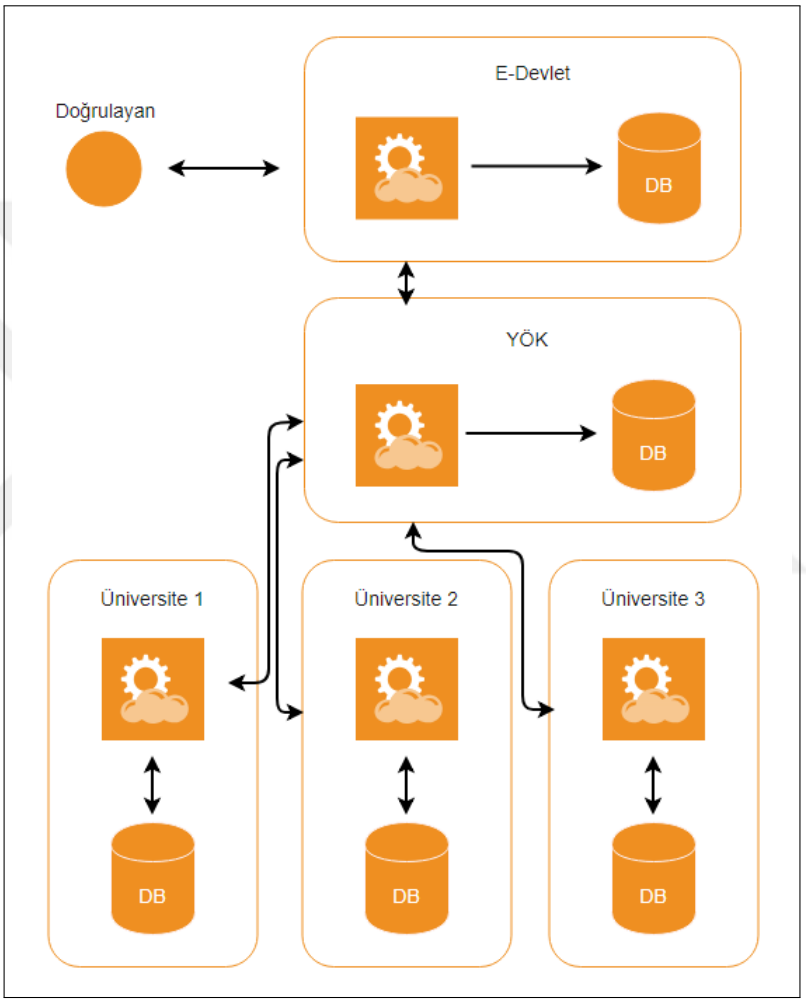
bağlantı üzerinden diploma numarası ile doğrulama yapmaktadır [24]. Üniversitelerin bu tür yaklaşımları ŞEKİL 2.3'deki gibi merkezi bir veri tabanı üzerinden sağlanmaktadır. Doğrulama işlemi işveren tarafında oldukça zaman almakta ve farklı farklı üniversitelerin farklı yaklaşımları sebebiyle yönetilmesi zor bir süreç olmaktadır.



Şekil 2.3: Üniversitelerin Diploma Doğrulama Mimarisi

İşverenler için farklı üniversite ve kurumlar ile doğrulama yapma zorluğu sebebiyle Qualificationcheck, EdX gibi özel çözümler doğmuştur [25, 26]. Farklı kurumların doğrulamasını tek çatı altından işverenlere sunulması fikrinden yola çıkarak farklı uluslardaki çeşitli yükseköğretim kurumlar ile anlaşarak geliştirdikleri web servisler ile işverenlere yetkinlik doğrulama hizmeti satmaktadırlar. EdX üzerinden yetkinlik kazanan bireylerin sertifikaları kolaylıkla doğrulanabilir ve paylaşılabilirdir. Bu platformlar kendilerine özel sertifikasyon süreçleri işletmekte ve üretilen diplomalarda standart uyumluğu bulunmamaktadır. Yeterliliklerin kontrolleri ve durumları merkezi bir yapı üzerinde tutulduğu için kalıcılık problemleri içermektedir. Bu da verinin bütünlüğü veya değiştirilip değiştirilmediği yönünden güvensizlik teşkil etmektedir.

Türkiye'de 2015 sonlarında geliştirilen E-Devlet üzerinden "Mezun Belgesi Sorgulama ve Doğrulama" çözümü ile Türkiye'deki yükseköğretim kurumlarından mezun olan kişilerin mezuniyet bilgilerinin temini ve doğrulaması yapılabilmektedir. YÖK'e bağlı kurumların mezun bilgilerini belli zamanlarda YÖK'e bildirilmekte ve belli dönemlerde veriler üzerinde mutabakat işlemleri gerçekleştirilmektedir. ŞEKİL 2.4 de görüleceği üzere YÖK'ün veri tabanlarına aktarması sonucunda toplanan verilerin merkezi E-Devlet platformu üzerinden doğrulaması yapılabilmektedir.



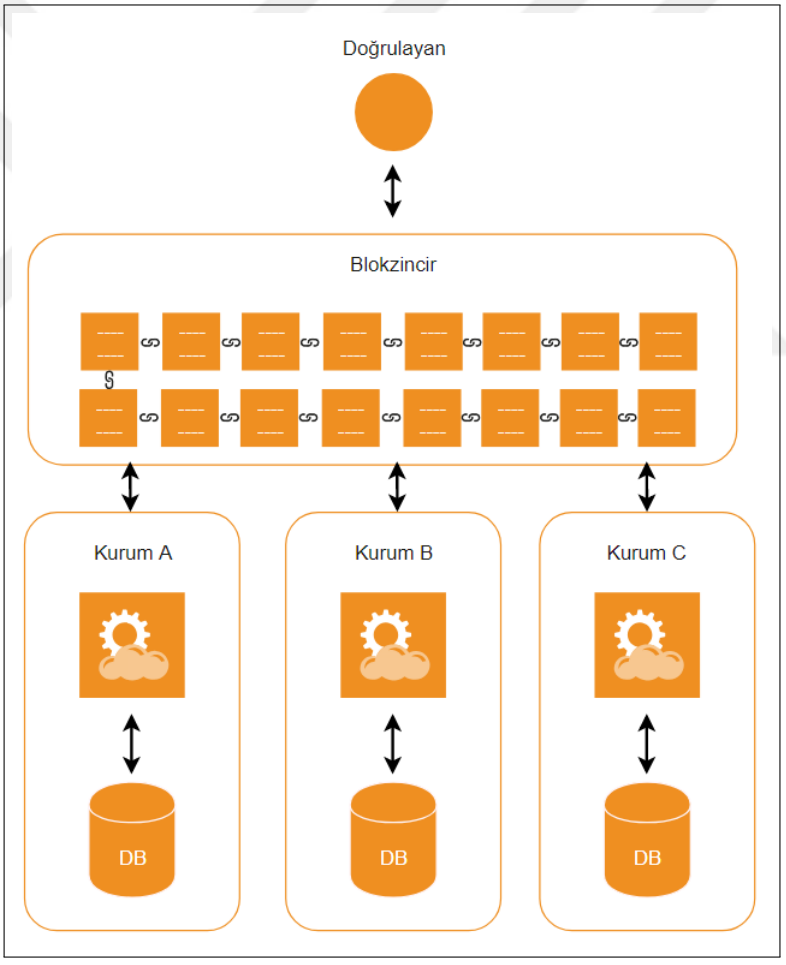
Şekil 2.4: E-Devlet Diploma Doğrulama Mimarisi

E-Devlet üzerinden çıkartılan diplomanın üzerinde kişi ve mezun olduğu kurum bilgileri dışında hızlı doğrulama imkanı sunan doğrulama bağlantısı bulunmaktadır. Bu bağlantı üzerinden E-Devlet sunucuları üzerinde doğrulama yapılabilmektedir [7]. Geliştirilen mobil uygulama sayesinde belge üzerindeki kare kod ile merkezi veri tabanları üzerinde doğrulama imkanı sunmaktadır [27]. Merkezi bir platformda sunulan bu yapı üzerinde yaşanacak problemler sonucunda veya veriler üzerinde yapılacak izinsiz değişiklikler ile

veri bütünlüğü ve kalıcılık problemleri söz konusu olabilmektedir. Buna ek olarak farklı uluslardan mezun olan bireylerin bu sistem üzerinden doğrulama yapması mümkün olmamaktadır. Bu kapsama giren bireylerin doğrulaması üniversiteler ve iş kurumları için problem teşkil etmektedir.

2.3.3 Dijital Merkezsiz Çözümler

Merkezi çözümlerin dışında merkezi olmayan yapılar üzerinde de diploma doğrulama imkanı sunan çözümler geliştirilmiştir. Merkezsiz ve dağıtık bir yapı sunan blokzincir mimarisi üzerinde diploma doğrulaması yapan çeşitli özel kuruluş ve üniversiteler bulunmaktadır.



Şekil 2.5: Merkezsiz Blokzincir Tabanlı Çözüm Mimarisi

- Sony Global Education firmasının sunduğu eğitim programlarının sertifikalarını blokzincir üzerinden doğrulama çözümü geliştirmişlerdir [28]. Global Math Challenge gibi programlarda kullanılmakta olan bu uygulama ile oluşturan sertifikaların PNG formatı üzerinden doğrulaması yapılabilmektedir. Bozulmuş veya manipüle edilmiş PNG sertifikalar sistem tarafından algılanmakta ve doğruluğu onaylanmamaktadır. Sony firmasının geliştirdiği çözümün, doğrulama adımlarını nasıl gerçekleştirdiğine dair açık bir kaynak doküman paylaşımı bulunmamaktadır.

- Coinfirm tarafından geliştirilen Trudatum çözümü ile dokümanların doğrulamasına olanak sağlamaktadır [29]. Doğrulamayı blokzincir üzerinden yapmakta ve her işlem için ücret almaktadır.

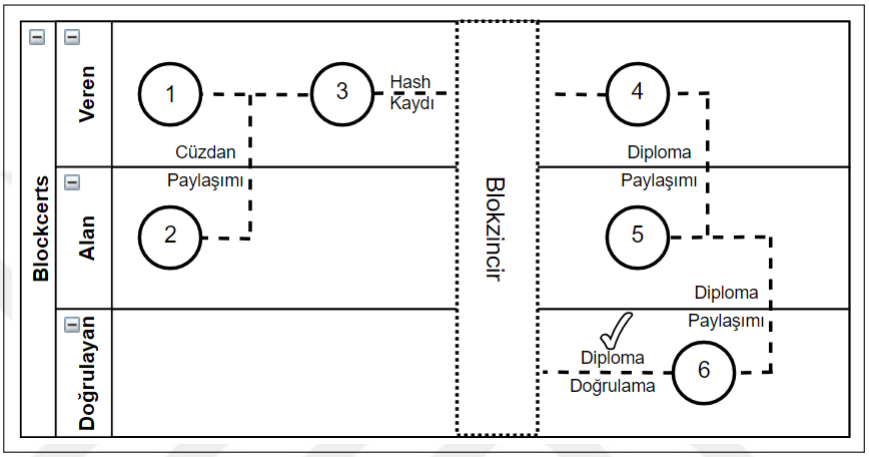
- Gradbase sayfasında her üç kişiden birinin CV'lerinde yalan söylediğini belirterek Bitcoin blokzinciri üzerinden beyan edilen yeteneklerin doğruluğunu kullanıcılarına sunmaktadır [30]. Bu çözümlerin standart uyumlulukları bulunmamakta ve doğrulama adımlarında kullandıkları yaklaşımların belirsiz olması sebebiyle güven problemi doğurabilmektedir.

- MIT lisanslı açık kaynak kodlu bir proje olan Blockcerts çözümü Open Badge standartlarına sahip JSON-LD formatındaki sertifikaların doğrulanması sürecini Bitcoin üzerinde gerçekleştirmektedir [12]. Diplomayı veren ve alanın Open Badge standartlarına göre tanımlandığı ve onaylama adımlarının açık bir şekilde gözlemlenebildiği bir yapı ortaya koymaktadır. Merkezi olmayan blokzincir yapısı üzerine kurulan Blockcerts uygulamasında diploma yayınlama, paylaşma ve doğrulama adımları yapılabilmektedir. Geliştirilen açık kaynak kodlu bu yapıyı birçok farklı üniversite kullanmaktadır [9, 31–33]

Blockcerts çözümünü üniversitelerin yapılarında kullandığını örneklemek adına MIT verilebilir. MIT Üniversitesi öğrencilerinin diplomalarını bu şekilde öğrencileri ile paylaşmakta ve doğruluğunu sağlamaktadır. İlk adım olarak öğrenciler diplomalarını alabilmek için üniversite ile kripto para cüzdan bilgilerini paylaşmaktadır. Üniversite öğrenciden temin ettiği bilgiler ve mezuniyet bilgilerini içeren dijital JSON formatta sertifika oluşturmaktadır. Oluşturulan sertifikanın özet değerini merkezsiz bir yapı olan Bitcoin blokzincir yapısı üzerinde kayıt altına almaktadır. Sonrasında blokzincir üzerinde özet değeri bulunan dijital diplomayı öğrencisi ile paylaşmaktadır. Dijital ortamda temin edilen

diploma öğrenci tarafından ihtiyaç halinde farklı üniversiteler veya iş kurumları ile paylaşılabilmektedir.

ŞEKİL 2.6 de gösterildiği gibi oluşturulan sertifikanın özet değerini merkezsiz bir yapı olan Bitcoin blokzincir yapısı üzerinde kayıt altına almaktadır. Sonrasında blokzincir üzerinde özet değeri bulunan dijital diplomayı öğrencisi ile paylaşmaktadır. Dijital ortamda temin edilen diploma öğrenci tarafından ihtiyaç halinde farklı üniversiteler veya iş kurumları ile paylaşılabilmektedir.



Şekil 2.6: Blockcert Akış Şeması

Kurumlar tarafından paylaşılan diplomanın herhangi bir yanlış veri içermediğini, diplomayı veren kurumu, diplomanın geçerliliğini ve manipüle edilip edilmediğini blokzincir üzerinde tutulan özet değer ile doğrulamasını hızlı ve güvenilir bir şekilde yapabilmektedir.

MIT geliştirmiş olduğu bu çözüm ile bünyesindeki diploma yönetimi sisteminin yanında daha güvenilir bir doğrulama mekanizmasını öğrencilerine sunmaktadır. Öğrencilerine ikinci bir diploma olarak JSON-LD formatında dijital diplomalarını paylaşmakta ve yüksek güven derecesi ile doğrulanmasını sağlamaktadır. Bu dijital diplomaların zincir üzerinde paylaşımı, bloklar içerisinde yer alması için Bitcoin uygulamasında tanımlı minimum işlem ücreti kadar ücret ödenmesi gerekmektedir. Blockcerts içerisinde ise bu varsayılan değer olarak 60,000 Satoshi yani 0.0006 BTC olarak tanımlanmıştır [34].

2.4 Metotların Karşılaştırılması

Bir önceki bölümde bahsedilen diploma doğrulama hususundaki çözüm metotlarının farklı özellikler üzerinde karşılaştırması TABLO 2.2'de özet bir şekilde gösterilmektedir.

TABLO 2.2: Farklı Çözümlerin Karşılaştırılması

Metot	Güven	Hız	İptal Edilebilirlik	Uyumluluk	Kalıcılık	Merkezsiz
Üniversite	Orta	Kötü	Evet	Evet	Hayır	Hayır
E-Devlet	Orta	İyi	Evet	Evet	Hayır	Hayır
Qualifica-tioncheck	Orta	Orta	Evet	Hayır	Hayır	Hayır
Gradbase	Orta	İyi	-	Hayır	Evet	Evet
Blockcerts	İyi	İyi	Evet	Kısmen	Evet	Evet

TABLO 2.2'de görüldüğü gibi E-Devlet çözümü uyumluluk açısından Türkiye'deki üniversitelerde sorun teşkil etmemekte fakat kalıcılık yönünden problemli noktalara sahiptir. Bunlara merkezi veri tabanı kullanımı ve manipülasyona açık veri barındırma ve doğrulama mekanizması gösterilebilir.

Karşılaştırma sonucunda uyumluluk dışında merkezsiz oluşu ve kalıcılığı sağlaması yönünden doğrulama mekanizması olarak Blockcerts kullanımı avantajlı gözükmektedir.

Blockcerts gibi bir yapı üzerinden doğrulama işlemlerinin gerçekleştirilmesini daha iyi görebilmek için SWOT/ GZFT analizi üzerinde de incelemesi yapılmıştır.

Güçlü:

- Maliyetler açısından verimlilik getirmesi,
- Kolay entegrasyon/uyum sağlanabilmesi,
- Herkesçe ve hızlı doğrulanabilir olması,
- Merkezsiz bir yapı olması,
- Güvenlik protokollerinin gelişmiş olması,
- Sürdürülebilir bir yapıya sahip olması.

Fırsatlar:

- Kalıcılığın üst seviyede olması,
- Uluslararası bir çözüm sunması,
- Güncel teknolojiyi yakalama fırsatı,
- Farklı kurumlar ile iletişim güvenliğinin artırması.

Tehditler:

- Çok fazla işlem, yük meydana gelebilmesi,
- Saldırgan kişilere çok açık olması,
- Yeni saldırı metotlarının geliştirilebilmesi.

Zayıf Yönler:

- Mevzuat ve bilgi yetersizliği,
- Yeni kavramlar içermesi.

Yapılan analiz gösteriyor ki blokzincir tabanlı merkezsiz mimariler evrak doğrulamasında önemli faydalar içermektedir. Fırsatlar ve güçlü yanları sebebiyle diploma yönetiminde kullanılması çok yararlı olmaktadır.

Bölüm 3

Blokzincir

Bu bölümde Türkiye'deki doğrulama sürecinde kullanmayı önerdiğimiz Blockcerts'in altyapısı olan blokzincir teknolojisi tarihi, mimarisi, özellikleri ve türleri başlıkları altında bahsedilmektedir.

3.1 Blokzincir Tarihi

Blokzincir ilk olarak 2008 yılındaki Satoshi Nakamoto takma adı altındaki makale ile sunulan Bitcoin uygulamasının altyapısı olarak blok ve zincir olarak ayrı ayrı tanımlanmış ve kullanımına 2009 yılında oluşturulan ilk blok ile başlanmıştır [1]. Sonralarında 2014 yılında Blokzincir 2.0 ile birlikte blok zincir uygulamaları tanımlanmaya başlanmıştır. Blokzincir; içerisinde çeşitli tiplerdeki verilerin içeren blokların eklemeli olarak birbirine bağlanması ile oluşmakta ve dağıtık yapıda bulunan düğümler arasında paylaşılmaktadır.

3.2 Blokzincir Mimarisi

Blokzincir içerisinde çok farklı katmanlar bulunduran bir çözümler bütünüdür. Bu nedenle fonksiyonellikler ve amaçlar doğrultusunda ayrıştırılarak incelenmesi gerekmektedir. Bu bölümde blokzincir uygulamaları mimari açıdan konsensüs, madencilik, yayılım, doğrulama ve uygulama olmak üzere beş katman hakkında kısaca bahsedilecektir [35]. ŞEKİL 3.1 de görüldüğü üzere blokzincir çözümleri öncelikli olarak güven yani konsensüs inşasını ele alarak katman katman oluşturulması gerekmektedir.

Şekil 3.1: Blokzincir Tabanlı Uygulamaların Katmanları

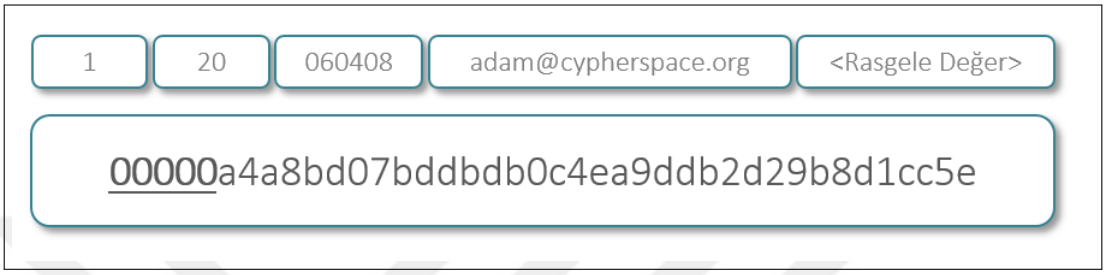
3.2.1 Konsensus Katmanı

Güven kavramını oluşturmak ve bir topluluğun aynı fikirde olmasının sağlanması oldukça zor problemlerden biridir. Özellikle bu durumu birbirini hiç tanımayan, isimlerinin dahi bilinmediği bir toplulukta inşa etmek kolay değildir. Blokzincirde de aynı bu ortam gibi birbirlerini tanımadan farklı nodeler - düğüm (noktalar) içermektedir. İşte bu ortamda blokzinciri oluşturan blokların format tanımlamalarının yapıldığı, yeni blokların oluşturulmasında ve doğrulanmasında farklı düğümler ile güvenin inşası için mutabakat protokolünün belirlendiği bölümü konsensüs katmanı olarak tanımlayabiliriz. [1]'deki Bitcoin uygulaması üzerinde Emek İspatı (Proof of Work) konsensüsü uygulanmaktadır. Bunun dışında sahip olduğu, cüzdanında bulunan miktari değerler kadar söz hakkı sunan Proof of Stake, harcama miktarı, elindeki parayı kaybetme riskini aldığı kadar güven veren algoritma olan Proof of Burn ve Proof of Space gibi çeşitli konsensüs yaklaşımları güvenin inşası için geliştirilmiştir [36–39].

Emeğin ispatı yaklaşımında güvenin inşası için belirli bir emeğin ortaya konulması gerekmektedir. Bu yaklaşım ilk kez spam maillerin önüne geçmek için göndericinin mail atmadan önce belirli bir efor ortaya koymasını gerektiren Hashcash çözümü ile karşımıza çıkmıştır [40]. Mail gönderen kişinin mail göndermeden önce "X-Hashcash" başlığı içerisinde yer alması gereken versiyon, bit adedi, tarih, alıcı, rasgele değer gibi değerler bütününü belirli bir kurala uygun oluşturması gerekmektedir. ŞEKİL 3.2 de gösterilen örnekteki gibi başlık içerisinde yer alan değerlerin SHA-1 özet çıktısının ilk 20 bit

değeri sıfır (0) olması gerekmektedir. Gönderen kişi uygun özet değerini bulmak için rasgele değeri artırarak denemeler yapmak ve CPU ile efor tüketmek zorundadır. Bu yaklaşım ile istenmeyen çoklu mail gönderimleri mail gönderimlerinin önüne geçilmesi düşünülmüştür.

X-Hashcash: 1:20:060408:adam@cypherspace.org::1QTjaYd7niiQA/sc:ePa



Şekil 3.2: X-Hashcash SMTP Başlık İçerik Örneği

Aynı emeğin ispatı yani Proof of Work protokolü yaklaşımı Bitcoin üzerinde zaman ve işlem hacmi gerektiren SHA-256 özet alma fonksiyonu üzerinden işletilmektedir [1]. SHA-256 hash almak oldukça kolaydır. Fakat fonksiyon çıktısının yani özet değerinin ne geleceğini bilmeden kurallara uygun bir formatta çıktı üretmek ise zor bir görevdir. Devam eden sürekli denemeler ile kurala uygun değer bulunmaya çalışılır. Bulma aşamasına kadar sürekli deneme gerçekleştirmek günümüz teknolojisi için yüksek CPU kaynak tüketimine karşılık gelmektedir. Talep edilen formattaki özeti elde etmek için çaba sarf etmek, ortaya emek koymak POW için güven inşasında anahtar rol oynamaktadır. Güveni inşa eden faktör ise SHA-256 özet algoritmasının geri döndürülemez şekilde tasarlanmasıdır. Çünkü özet fonksiyonları geriye döndürülemez ve özetten ana metin tahmin edilemezdir [41]. Herhangi bir saldırgan şuan ki teknoloji ile emeksiz kurallara uygun özet değer üretmesi mümkün değildir.

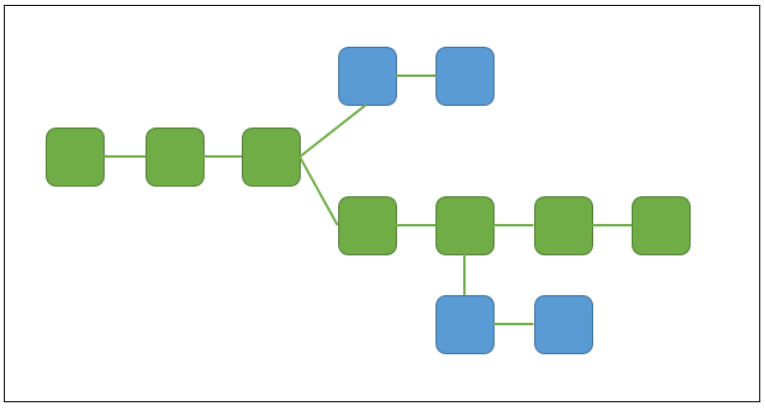
3.2.2 Madencilik Katmanı

Blokzincir yapısının, üzerinde koşan uygulamaların sürdürülebilir olması için yeni blokların onay sürecinden geçip sisteme yani blok zincire dahil olması gerekmektedir. Yeni blokların doğruluğu onaylanır ve mevcut zincire eklenirse sistem ilerleme gösterir ve Bitcoin gibi uygulamalarda yeni para transferleri gerçekleşir. Bunun için de blokların

doğrulanması ve zincire eklenmesi görevini üstlenen düğümlere ihtiyaç vardır. Blokzincir bünyesine yeni blokların eklenmesi için her zaman düğümlere ihtiyaç duymaktadır. Herkese açık blokzincir yapılarında düğümlerin sisteme dahil edilmesi için teşvik protokolü bu katman üzerinde ele alınabilir. Bitcoin sisteminin teşvik yapısını inceleyecek olursak madenciler yani düğümler her onayladıkları blok için belli bir miktar bitcoin almaktadırlar. Bulunduğumuz yıl içerisinde bloğu doğrulayan düğümlere 12.5 BTC dağıtımı yapılmaktadır. Madencilerin aldığı bitcoin miktarı her 4 yılda bir yarı yarıya azaltılmakta böylelikle alınan bitcoin miktarı ile değeri arasında denge kurulmaktadır. Ek olarak blok içerisinde yer alan her işlemden de teşfik primi düğümlere dağıtılmaktadır. Böylelikle yeni işlemleri içeren yeni bloklar doğrulanmakta ve zincire eklenmektedir. Zincire ekleme işlemi ile birlikte blok içerisinde ki para transferi işlemleri gerçekleşmiş manasına gelmektedir. Madencilik katmanında tanımlanan bu tarz politikalar ile madencilere kazanç sağlanmakta ve sistemin sürdürülebilir olması sağlanmıştır.

3.2.3 Dağılım ve Transfer Katmanı

Bir blokzincirde hangi zincirin ana zincir olduğuna karar vermek ve bağımsız hareket etmemek, kopmamak ve aynı zamanda yeni blok üretiminde bu bilgiyi diğer bloklara iletmek gerekmektedir. Bu hususta düğümler arası iletişim oldukça önemlidir. Düğümler arasında ana zincir dışında yeni bloklar keşfedildikçe yan zincirler oluşmakta fakat iletişim ve karar mekanizması sebebiyle daima tek bir ana zincir korunmaktadır. İki madencinin benzer zamanlarda blok üretilmesinden kaynaklı kullanım dışı kalan fakat geçerli blokları içeren zincirlere yetim/stale blok denilmektedir[42, 43]. Tanımlanan karar mekanizması sayesinde daima tek zincir üzerinden yapı ilerletilmektedir.



Şekil 3.3: Ana ve Yetim Zincir Gösterimi

3.2.4 Doğrulama Katmanı

Blokzincirde üretilen yeni blokların önceki bloklar ile ne şekilde bağlanması gerektiğinin yanı sıra üretilen bu bloğun içerisindeki verini formatının uygunluğunu belirleyen protokoldür [1, 42]. Bitcoin blok zincirindeki blokların boyutu 1 MB olacak şekilde sınırlandırılmıştır ve TABLO 3.1 de gösterildiği başlık değerlerini barındırması gerektiği tanımlanmıştır.

TABLO 3.1: Bitcoin Blok Başlıklarının Örnek Gösterimi

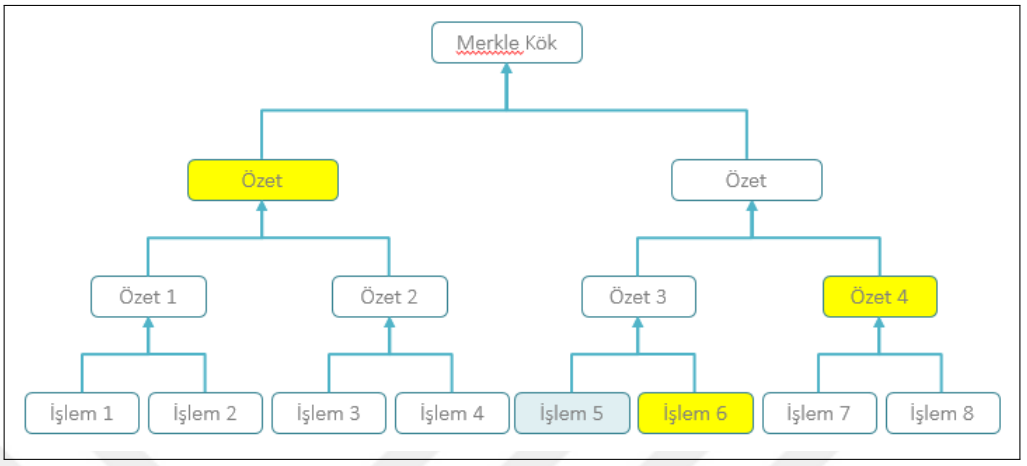
BLOCK	123456
Hash	0000000000002917ed80650c6174aac8dfc46f5fe36480aaef682ff6cd83c3ca
Previous Block	0000000000000b60bc96a44724fd72daf9b92cf8ad00510b5224c6253ac40095
Time	May 12, 2011 2:46:46 PM
Difficulty	157416.40184364
Number Of Transactions	13
Block Reward	50 BTC
Size	4179
Nonce	2436437219
Merkle Root	0e60651a9934e8f0decd1c5fde39309e48fca0cd1c84a21ddfde95033762d86c

- Hash; Blokzincir çözümlerinde bloklar arası bağlantı özet değerler üzerinden sağlanmaktadır. Yeni oluşturulacak blok ile mevcut ana zincir bağlantısının kurulması için içeriğinde bir önceki bloğu temsil eden özet değerin bulundurulması germektedir. Zincirin devamlılığının doğrulanması için bu değer kullanılmaktadır.

- Nonce; Blok başlık tanımlarında yer alan nonce değeri ise madencilik sürecinde "özet değerinin ilk 20 biti sıfır olacak" şeklinde olabilen kurallara uygun blok özetinin bulunması için madenci tarafından değiştirilen rasgele bir değerdir. Bu rasgele değer madenci tarafından doğrulama adımında devamlı değiştirilmekte ve kurallara uygun blok özet değeri tespit edilmesi ile birlikte son kullanılan bu rasgele dijit değer nonce olarak blok içerisinde kayıt altına alınmaktadır. Madencinin bulmuş olduğu özet değerin doğruluğunu bu nonce değerler hesaba katılarak doğrulanmaktadır.

- Merkle Root; Blok içerisinde yer alan para transfer işlemlerinin hızlı bir şekilde doğrulanması için madenci tarafından Merkle kökü hesaplanarak kayıt altına alınmaktadır. Böylelikle network içerisinde işlemlerin doğrulama süreci hız kazanmaktadır. ŞEKİL 3.4 de gösterilen örnek şema üzerinde "İşlem 5" işleminin doğruluğunu hesaplamak için sarı olan değerlerin paylaşılması doğrulama için yeterli

olmaktadır. Bu algoritma kullanılarak güvenilir bir şekilde hem yer tasarrufu hem de işlem hızı kazandırmaktadır [44].



ŞEKIL 3.4: Merkle Root Hesaplama Şeması

3.2.5 Uygulama Katmanı

Daha önce bahsedilen dört katman üzerine inşa edilmiş ve belirli işlemlerin gerçekleştirildiği katmak olarak uygulama katmanını inceleyebiliriz. Para transferi ya da talep edilen bir fonksiyonun gerçekleştirildiği katmandır. Bitcoin blokzincir blokları içerisinde yer alan işlemlerin nasıl, ne formatta bulunması gerektiği tanımları yapılmakta ve gerekli uygulamalar bu yapı üzerinden işletilmektedir. TABLO 3.2'de örnek Bitcoin işlem içeriğinde görüleceği üzere uygulama için gerekli tüm işlem parametrelerin tanımlanan formatta yer alması gerekmektedir. Farklı uygulamalar için içerik paylaşımı, görüntüleme gibi fonksiyonellikleri sunan servis çağrımları bu standartlar üzerinden sağlanmaktadır [45, 46].

TABLO 3.2'de gösterilen Bitcoin işlem yapısı güvenlik ve doğrulama hızını artırma açısından birçok değişkeni içerisinde barındırmaktadır. Aynı zamanda Bitcoin işlem yapısında girdiler ve çıktılar şeklinde farklı değişken tiplerini bünyesinde barındır.

- Previous Tx Hash: Yeni gerçekleştirilecek işlem içerisinde daha önce gerçekleştirilmiş işlemin özet değeri girdi olarak tutulmaktadır.
- ScriptSig: Farkı cüzdanlardaki paraların harcanmamasını sağlayan önemli bir alandır. Burada işlem yapacak kişinin kendisinin bu tutarı kullanmaya yetkisinin olduğunun ispatını bu alan üzerinden sunmaktadır.
- ScriptPubKey: Geçerli bir işlem için işlem içerisinde belirtilen tutarı kimin kullanabileceğinin koşulu yer almaktadır. İşlem içerisinde aktarılan BTC'yi ancak bu koşulu sağlayabilen cüzdan sahibi kullanabilmektedir.

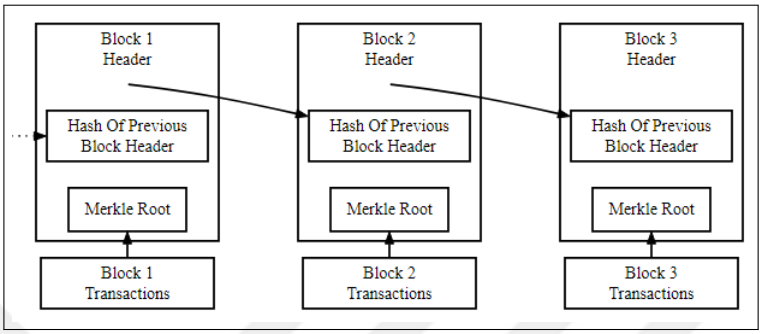
Bitcoin işlemi içerisindeki çıktının geçersiz olduğunu belirtmek için ScriptPubKey alanında OP_RETURN işaret bayrağı kullanılmaktadır. Bu işaretleme işlemi 32 byte büyüklüğünde keyfi kullanıma açık bir alan barındırmaktadır. Bu alan Blockcerts gibi para transferi dışında birçok uygulama tarafından kullanılmaktadır [12, 47, 48].

Tablo 3.2: Bitcoin İşlem Yapısı

Version	01 00 00 00
Number of Inputs	01
Previous Tx Hash	41 6E 9B 45 55 18 0A AA 0C 41 70 67 A4 66 07 BC 58 C9 6F 01 31 B2 F4 1F 7D 0F B6 65 EA B0 3A 7E
Previous Output Index	00 00 00 00
Script Lenght	6A
ScriptSig	47 30 44 02 20 LC 3B E7 LE 17 94 62 LC BE 3A 7A DE CI OF 25 F8 18 F2 38 F5 79 6D 47 15 21 37 EB A7 10 F2 17 4A 02 20 4F 81 E6 67 B6 96 E3 00 12 OF 4E 56 AC 96 OF B8 30 BD DF FE E3 BL 5D 2E 47 40 66 AB 3A A3 9B AD 01 21 03 BF 35 OD 28 21 37 51 58 A6 08 B5 LE 3E 89 8E 50 IF E4 IF 2D 2E 8C 77 4D E4 A9 A7 ED EC F7 4E DA
Sequence	FF FF FF FF
Number of Outputs	01
Value	20 4E 00 00 00 00 00 00
Script Length	19
ScriptPubKey	76 A9 14 E8 LD 74 2E 2C 3C 7A CD 4C 29 DE 09 OF
Locktime	00 00 00 00

3.3 Blokzinciri Önemli Yapan Özellikler

Blokzincir verileri belli ebatlarda bloklar halinde saklamaktadır. Bu bloklar birbirine bağlanarak büyümekte olup, yeni oluşan blok kendisinden bir önceki bloğun SHA-256 özet değerini barındırarak zincir oluşmaktadır.

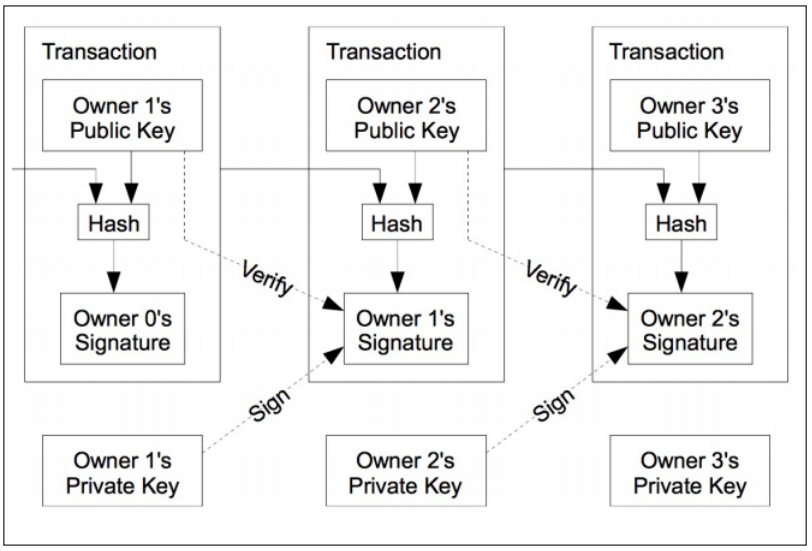


Şekil 3.5: Bitcoin Bloklarının Bağ Gösterimi [1]

Blok içerisindeki bir verinin herhangi bir karakterindeki değişim uygun blok özet değerinin tekrardan hesaplanması için ek çabaya sebep olacaktır. Bu bloğun özetini içerisinde barındıran devam bloklarında da tekrardan hesaplamaya gidilmesi gerekmektedir. Bloktaki bu değişimin hiçbir düğüm tarafından fark edilmemesi, ağ içerisinde geçerli olması yani tüm düğümler tarafından kabul görmesi için kendisinden sonra oluşan tüm blokların özet değerlerinin tekrardan hesaplanması gerekmektedir. Bu işlemi de aynı zamanda tüm düğümlerin işlem hızlarından daha hızlı gerçekleştirmek zorundadır. Emeğin ispatı mutabakat yaklaşımın da ana düğümdeki bu blokların hepsinin değişimi mevcut teknoloji ile yüksek maliyet yani emek ve zaman gerektirmektedir.

Mevcut teknolojiler ile zincirin kurallarını bozmadan blok içerisindeki verilerin değiştirilmesindeki zorluk sebebiyle blokzincir içerisindeki veriler değiştirilemez kabul edilmektedir [1].

Bitcoin'de ECDSA algoritması kullanılarak sayısal imzalar üretilmekte ve bu imzalar ile işlemler gerçekleştirilmektedir. Algoritma sonucunda ortaya çıkan rasgele sayılardan oluşan açık anahtar üzerinden aynı zamanda Bitcoin adresi de üretilmektedir [49]. Bu bilgiler herkes tarafından bilinmekte fakat bu veriler üzerinden gizli anahtar mevcut teknoloji ile elde edilememektedir. Üretilen gizli anahtar ise başkaları tarafından ele geçirilemez olması gerekmektedir. Bu durum korunduğu müddetçe günümüz teknolojisinde gizli anahtarlar üzerinden gerçekleştirilen işlemlerin taklit edilmesi oldukça zordur. Bu



Şekil 3.6: Bitcoin İmzalama ve Doğrulama İşlemleri [1]

yaklaşım ile blokzincirdeki işlemin kimler tarafından gerçekleştirildiği, sahipliği net bir şekilde tespit edilebilmektedir. Bitcoin gibi yapıları açık olarak tasarlanan blokzincir yaklaşımları sayesinde gerçekleştirilen blok işlemleri her görüntüleyen tarafından erişilebilir konumda olmaktadır. Dileyen herkes bir açık blokzincir içerisinden hangi adres, hangi adrese ne kadar BTC göndermiş görebilmektedir.

3.4 Kayıt Edilebilen Data Türleri

Çoğunlukla işlem bilgisi ve akıllı sözleşmeler blokzincir içerisinde kayıt altına alınmaktadır. Fakat yeni yaklaşımlar ile Bitcoin içerisindeki yazılabilir alanlara sertifika, belge özetleri yanında birden fazla işlemler ile dosya, resim veya zararlı dahi eklenebilmektedir [47]. İşlem bilgisi olarak farklı yaklaşımlar mevcuttur. Bunlardan en popüleri kripto para birimlerinin alıcı ve verici arasında aktarıldığı BTC transfer işlemleridir. Farklı olarak sertifika veren kurum ile sertifikayı alan alıcı arasında varlık transferinin gerçekleştirilmesi işlemidir. Bu yaklaşım ile alıcının, transfer edilen varlığa sahip olduğunun ve tüm haklarının alıcıya aktarıldığının ispat edilmesi amaçlanmıştır [12, 48]. Diploma doğrulamada bu yaklaşım uygulanmaktadır. Aynı zamanda akıllı sözleşmeler diye belirtilen farklı uygulamalarda mevcuttur. Belirli koşullarda ve ücret karşılığında çalıştırılabilecek

küçük programların yani sözleşmelerin blokzincir üzerinde tutulması olarak tanımlanmaktadır. Dışarıdan bu sözleşmeler çağırılarak belli başlı işlemlerin gerçekleştirilmesine olanak tanınmaktadır [46].

3.5 Blokzincir Ağ Türleri

Blokzincir yapıları düğümlerden oluşmakta ve bu düğümlerde tutulan veriler görüntülenebilmektedir. Bu iki kavramdaki kısıtlamalar ile kullanım alanlarına göre blokzincirler dört türe ayrılmış olarak tanımlanmaktadır [50].

3.5.1 İzinsiz Açık Blokzincir

Bitcoin gibi yapılarda herkes düğüm olabilir. Yetkili diye bir kavram yoktur. Bu sebepten Bitcoin altyapısı izinsiz olarak sınıflandırılmıştır. Bunun yanında bloklar içerisinde tutulan işlem bilgilerinin herkes tarafından görüntüleniyor olması sebebiyle açık olarak tanımlanmaktadır. Önceki bölümlerde de bahsedildiği gibi Bitcoin içerisinde gerçekleştirilen her işlem hangi adres tarafından hangi adrese ne miktarda BTC transfer edilmiş her kullanıcı tarafından açık bir şekilde sorgulanıp, doğrulanabilmektedir. Bu özelliği sayesinde doğrulama mekanizmaları için güvenilir, ortak bir ortam sunmaktadır.

3.5.2 İzinsiz Gizli Blokzincir

Bloklar içerisindeki verinin herkesçe onaylanıp, doğrulanıp yeni bloklar oluşturabildiği fakat herkesçe anlaşılıp, okunamadığı altyapılar izinsiz gizli blokzincir türlerine girmektedir. Zcash bunlara örnektir. Bu tarz blokzincirlerde zero-knowledge gibi ileri kriptolama algoritmaları kullanılmaktadır [51].

3.5.3 İzinli Açık Blokzincir

Ripple gibi zincirdeki düğümlerin belli onaylar, izin protokolleri çerçevesinde belirlendiği fakat blok içeriği herkesçe erişilebilir olan blokzincirler izinli açık blokzincir türü olarak tanımlanmaktadır.

3.5.4 İzinli Gizli Blokzincir

Hyperledger gibi bazı kurumların kendi yapıları için veya bankalar arasında gerçekleştirdiği örnek çalışmalarda uygulanan, düğümlerin belli politikalarla belirlendiği ve blok içeriklerinin herkesçe okunamayan blokzincir türlerine izinli gizli blokzincir denilmektedir.

Bölüm 4

Blockcerts

Karşılaştırma bölümünde de değindiğimiz Blockcerts çözümünü sağlamış olduğu fonksiyonlar ile birlikte bu bölümde detaylandırılmıştır. Çözüm, bünyesinde ŞEKİL 2.6'de görüldüğü üzere diploma oluşturma, yayınlama, paylaşma ve doğrulama fonksiyonlarını barındırır. Her bir fonksiyonda gerçekleştirilen standartlar bu bölümde incelenmiştir.

4.1 Dijital Diploma Oluşturma

Bireye yetkinlik kazandıran ve bunun karşılığında diploma veren kurumun diploma bilgilerini ve alıcıyı tanımlayıcı bir karakter dizisine ihtiyacı vardır. Bunun için de alıcılardan cüzdan bilgilerini temin etmesi gerekmektedir. Bu diploma ve alıcı bilgiler üzerinden açık kaynak kütüphane olan Cert-tools modülü ile JSON-LD formatında henüz imzalanmamış, blokzincire aktarılmamış dijital diplomaları oluşturulur. Bu adım ile her bir diploma için bir JSON dosyası oluşturulmakta ve dosya sistemi üzerinde muhafaza edilmektedir. Diploma doğrulama adımında kullanılan Context alanında belirtilen standartlara uyum olmalıdır. TABLO 4.1'de gösterilen örnek de görüldüğü gibi IMS Open Badge ve Blockcerts json standartları dijital diploma içerisinde kullanılmaktadır. Aynı zamanda ihtiyaç duyulan ek alanlar için de bu context içerisine ilgili standart kullanımın belirtilmesi gerekmektedir. Standartlar içerisinde diplomayı yayınlayan kurumun ve yeterliliği kazanan bireyin kimliği , blokzincir anahtarı, doğrulama için gerekli özet değerleri ve diploma iptali yönetimi gibi çözümleri barındırmaktadır.

Tablo 4.1: İmzalanmamış Dijital Diploma

```
{
  "id": "",
  "issuedOn": "2019-01-01T01:01:01.000000+00:00",
  "recipient": {
    "identity": "example@example.org",
    "type": "email",
   "hashed": false
  },
  "type": "Assertion",
  "verification": {
    "publicKey": "ecdsa-koblitz-pubkey:<publickey>",
    "type": [
      "MerkleProofVerification2017",
      "Extension"
      ]
  },
  "@context": [
    "https://w3id.org/openbadges/v2",
    "https://w3id.org/blockcerts/v2"],
  "displayHtml":"",
  "badge": {
    "issuer": {
      "url": "https://www.issuer.org",
      "name": "University",
      "email": "contact@issuer.org",
      "type": "Profile",
      "id": "https://www.issuer.org/issuer.json",
      "image": "",
      "revocationList": "https://www.issuer.org/revocation_list.json"},
    "name": "Certificate of Accomplishment",
    "type": "BadgeClass",
    "criteria": {"narrative": ""},
    "image": "",
    "id": "urn:uuid:82a4c9f2-3588-457b-80ea-da695571b8fc",
    "description": "",
    "signatureLines": [
        { "jobTitle": "University Issuer",
          "name": "Signature",
          "type": [
                    "SignatureLine","Extension"
                  ],
          "image": ""}
     ]
  },
  "recipientProfile": {
    "publicKey": "ecdsa-koblitz-pubkey:<publickey>",
    "name": "<name>",
    "type": ["RecipientProfile","Extension"]
  }
}
```

4.2 Dijital Diploma İmzalama ve Yayınlama

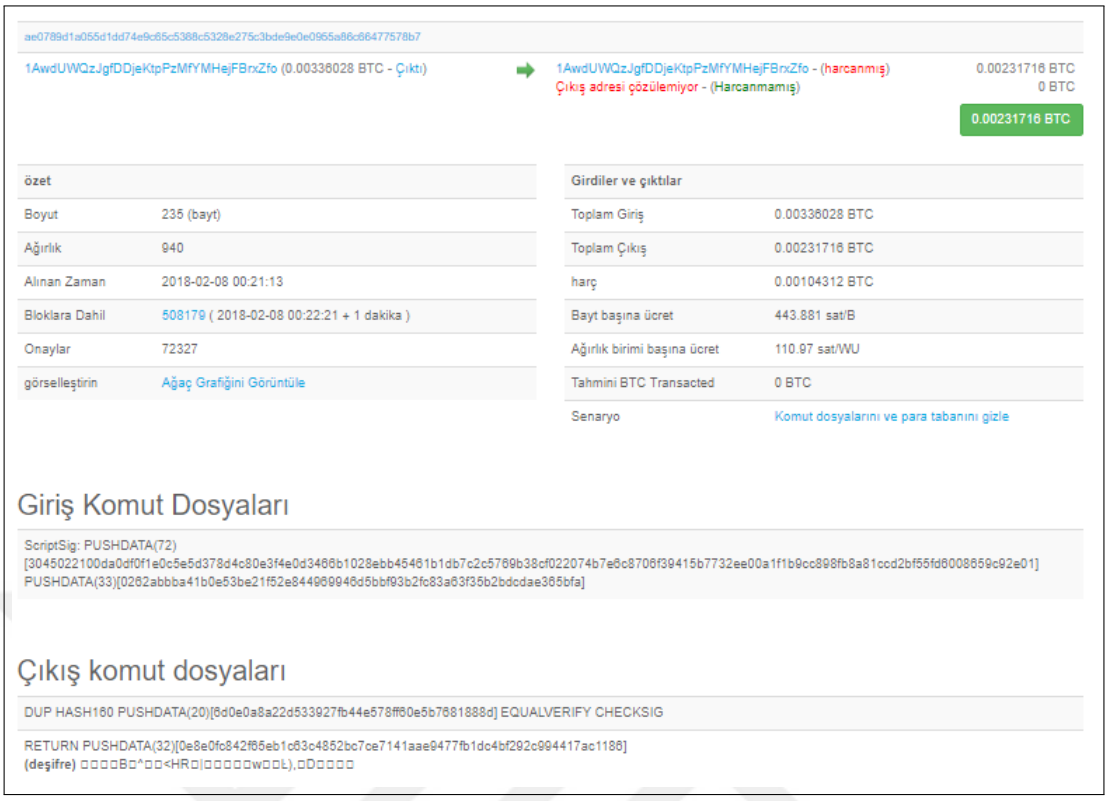
İmzalanmamış belirli standartlara uygun JSON formattaki dijital diploma Cert-issuer kütüphanesi ile imzalanarak Bitcoin işlemi içerisinde yer alan ScriptPubKey değerinde OP_RETURN bayrağı ile diploma özeti eklemesi yapılarak blokzincir üzerinde Bitcoin işlemi gerçekleştirilir. İlgili işlemi içeren bloğun doğrulanması ile blokzincir üzerinde diploma özeti kayıt altına alınmış olur. Diploma doğrulama adımında kullanılmak üzere

imzalanan JSON içeriğine TABLO 4.2'de gösterilen kayıt altına alınan işlem bilgileri ile birlikte ispat alanları yerleştirilir. Bu yayınlama işlemi her bir diploma için yapılabildiği gibi, tek bir Bitcoin işleminde birden fazla diploma da yayınlanabilmektedir. Bu yöntem için imzalamada sırasında farklı diplomaların özet bilgileri Merkle Tree algoritmasından geçirilmekte ve bu şekilde kullanılmaktadır [34, 44].

TABLO 4.2: İmzalanmış Diplomanın Ek Alan İçeriği


```
"signature": {
    "type": [
      "MerkleProof2017",
      "Extension"
    ],
    "merkleRoot": "0e8e0fc842f65eb1c63c4852bc7ce7141aae9477fb1dc4bf292c994417ac1186",
    "targetHash": "fedc56cf379c03aafbed63e592780a65bf9bbb43b749ac377a4fc6d2a36965d8",
    "proof": [
        {
          "right": "e577b05b66a6598d6264e9765e016fcc50b05eba0d5a2f6a339fad3983c7a629"
        },
        {
          "left": "e2effbdf969f1121b27850abd68718ad4e3f86658d8dfffdb5b9e67b007dfd0c"
        },
        {
          "right": "3e863b587b4303654d55fb24b469f3fdcaa9ffe325766596d462cde5144ab549"
        }
    ],
    "anchors": [
      {
        "sourceId": "ae0789d1a055d1dd74e9c65c5388c5328e275c3bde9e0e0955a86c66477578b7",
        "type": "BTCOpReturn","chain": "bitcoinMainnet"
      }
    ]
```


- type alanı içerisinde özet değer oluşturmada ve doğrulamada kullanılan standartlar belirtilmektedir.
- merkleRoot alanı diplomanın doğrulama ana özeti olup blokzincir üzerinde kayıt altına alınan değeri içermektedir.
- targetHash alanı ilgili diplomanın özetini belirtmektedir. Diplomanın değiştirilmediği bu bilgi üzerinden doğrulanmaktadır.
- proof alanı ile Merkle Tree doğrulamasının yapılabilmesi için ihtiyaç duyulan left, right ek özet değerleri paylaşılmaktadır.
- anchors.type alanında doğrulamanın yapılacağı zincir bilgisi yer almaktadır.
- anchors.sourceId alanı diplomanın zincir üzerinde yayınlanan işlem kimliğini göstermektedir. ŞEKİL 4.1'de gösterilen işlem içeriğine bu alan üzerinden erişilmektedir.



Şekil 4.1: Diploma Özeti İçeren İşlem Detayları

4.3 Dijital Diploma Paylaşımı

Üretilen imzalanmış diplomanın paylaşımı mail gibi farklı kanallar üzerinden paylaşılabildiği gibi, kurumun sunmuş olduğu portal linki üzerinden de diplomayı alan kişi bu diplomaya erişip Blockcerts tarafından geliştirilen android veya ios mobil uygulamalar ile diplomalarını bir platform üzerinde toplayabilmektedir [52]. Diploma paylaşımı kurumdan, yetkinlik kazanan bireye olduğu gibi aynı zamanda yetkinliğini ispatlamak isteyen bireyden, farklı kuruluşlara da yapılabilmesi gerekmektedir. Geliştirilen mobil cüzdan sayesinde paylaşım farklı kanallar ve uygulamalar üzerinden yapılabilmektedir. Oluşturulan JSON-LD formatındaki diplomalar içerisindeki diplayHTML alanı ile kuruma özel tasarlanabilmekte ve böylelikle insan gözüyle daha okunabilir bir formatla gösterilebilmektedir.

4.4 Dijital Diploma Doğrulama

Blockcerts üzerinde barındırdığı format, özet değer ve diploma durumu doğrulama olarak üç farklı kategorideki kontrol adımları ile diploma doğrulaması gerçekleştirmektedir.

Format doğrulama,

- JSON-LD Standartlarına uyguluk kontrolü,
- Onaylanmış blokzincir işlemi tespiti,
- Diploma özet değeri kontrolü,
- Zincir üzerinden özet değer temin edebilme,
- Yayınlayan kuruluşun kimlik kontrolü,
- Kurulusun anahtarları kontrol edilmektedir.

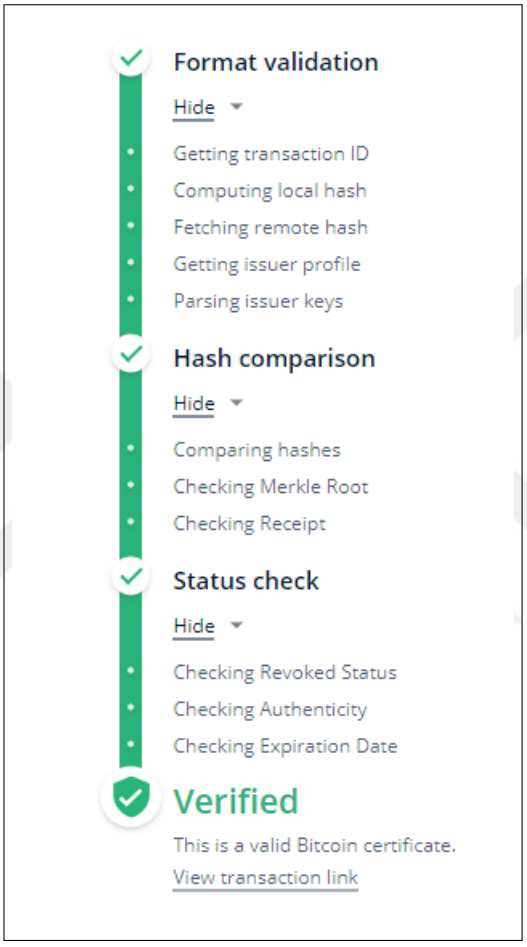
Özet değer doğrulama,

- Blokzincirdeki özet değer karşılaştırması,
- Merkle Root özet değerleri kontrolü,
- Alıcı kontrolü yapılmaktadır.

Durum kontrolleri,

- Diploma iptali kontrolü,
- İşlemin yetki doğruluğu tespiti,
- Anahtarların geçerliliğinin doğrulaması yapılmaktadır.

Diplomanın format kontrolü akabinde diploma özeti ve imza alanındaki Bitcoin işlem belirtecindeki OP_RETURN değeri ile karşılaştırılmaktadır. Karşılaştırma doğru ise veren ve alan kimlik birlikleri kontrol edilerek, diplomanın geçerlilik süresi , iptal durumu doğrulaması ile işlem tamamlanmaktadır. Uygulama bünyesinde geliştirilen Cert-Verifier kütüphanesi açık kaynaklı olup doğrulama adımlarını şeffaf bir şekilde gerçekleştirme kapasitesine sahiptir.



Şekil 4.2: Blockcerts Doğrulama Adımları

Bölüm 5

Türkiye'de Diploma

Bu bölümde Türkiye'deki farklı üniversitelerce uygulanan diploma yönetmelikleri analiz edilmiştir. Diploma içeriklerinin kullanım oranları çıkartılarak Türkiye diploma ihtiyacı ortaya konmuştur. Bunu yanında AB standardı olan diploma ekinin içeriği incelenerek Blockcerts üzerinde uyumluluk çalışması yapılmıştır.

5.1 Kullanımdaki Diploma Alanlarının Çıkartılması

Türkiye'de diploma üretiminde YÖK tarafından sadece kişinin kayıtlı olduğu enstitü anabilim/ana sanat dalındaki programın onaylanan program ismi ile yayınlamasını istemektedir. Bunun dışında her üniversite kendi diploma yönetmeliğine göre davranmaktadır.

Tablo 5.1: Diploma Alanlarının Kullanım Oranı

Diploma No	%100	Mezuniyet Tarihi	%100	Öğrenci Soyad, Ad	%100
Diploma Derecesi	%100	Düzenleme Tarihi	%50	Öğrenci No	%45
Üniversite Adı	%100	Kayıt Tarihi	%10	Ana/Baba Adı	%70
Anabilim Adı	%100	Mezuniyet Notu	%20	Doğum Yeri/Tarihi	%70
Diploma Eki	%100	Tez/Proje Başlığı	%5	TC/Pasaport No	%95

Çalışma kapsamında Türkiye'deki 20 üniversitenin diploma yönetmelikleri incelenmiştir [53–72]. TABLO 5.1'de görüleceği üzere bu yönetmelikler içerisinde diplomada yer alan bilgilerin kullanım oranları çıkartılmıştır. Bu çalışma ile kullanım oranları üzerinden Türkiye üniversitelerinin ihtiyaç duyduğu diploma nitelikleri belirlenmiştir.

5.2 Diploma Eki

Türkiye'deki üniversitelerin uluslararası şeffaflığının artırılması, mezunların elde edindikleri beceri, yeti ve kabiliyetlerin ifade edildiği, ulusal düzeyde anlaşılır akademik ve mesleki tanınmanın artırılması ile iş bulma imkanının sağlanması ve tüm Avrupa'da kabul gören ortak diploma oluşturma amacıyla yükseköğretim diploması yanında diploma eki verilmektedir [14–16]. Ulusal kurumlar tarafından kabul edilmiş, UNESCO, Avrupa Konseyi, Avrupa Komisyonu ile beraber belirlenen bir şablona göre diploma eki düzenlenmektedir. Bu kapsamda oluşturulan diploma eki içeriği aşağıdaki verileri içeriyor olması gerekmektedir.

- Kişi: Ad-soyadı, doğum tarihi, öğrenci no.
- Yetkinlik: Adı, ana alanı, kurumun adı ve statüsü, öğrenim dili.
- Yetkinlik düzeyi: Düzeyi, süresi, kabul edilme koşulları.
- Programın içeriği ve sonuçları: Programın türü, detaylı bilgi, alınan dersler/notlar/krediler, notlandırma, yetkinliğin sınıfı.
- Yetkinliğin kullanım alanları: Üst dereceye başlama imkanı, meslek icra etme hakkı.
- Ek bilgiler: Ek bilgi ve elde edilebilecek başka kaynaklar.
- Tasdik: Resmi tasdik içermelidir.

> "Tüm dünyada yeni diploma ve sertifikasyon şekilleri gelişmekte; hızla değişen iktisadi, siyasal ve teknolojik gelişmeler karşısında ülkeler öğrenci başarı değerlendirme tarz ve eğitim sistemlerini sürekli olarak değiştirmektedir. Sayıları hızla artan hareketli yurttaşlar, yeti ve becerilerinin adil değerlendirmesini talep etmektedir. Yeti ve becerilerin tanınmaması ya da yanlış veya eksik değerlendirilmesi küresel bir sorun haline gelmiştir. Orijinal diploma ve diğer belgeler kendi başlarına yeterli açıklayıcı bilgi arz etmediklerinden dolayı, ayrıntılı ek açıklama tedarik etmeden bir diplomanın düzey ve işlevini kabul ettirmek son derece güç hal almıştır. Diploma Eki bu zorluklara cevaben üretilmiştir;
>
> - Yükseköğretimde saydamlık sağlar.
> - Diploma gibi eğitim belgelerinin süratle dikkate alınmasını sağlar.
> - Hareketliliği kolaylaştırır; yaşam boyu eğitimi ulaşılabilir kılar.
> - Sahip olunan diploma ve beceriler hakkında adil, güvenilir ve yetkin bilgi verir.",

İfadesiyle diploma ekinin gereksinimi dile getirilmiştir [73].

Bölüm 6

Türkiye'de Blokzincir Tabanlı Diploma Yönetimi

Analiz neticesinde Türkiye'de diploma üretiminde ihtiyaç duyulan nitelikler ile merkezsiz bir yapıda doğrulama imkanı sunan Blockcerts'in sertifika içerikleri karşılaştırılmıştır. Bu karşılaştırma sonucunda ek ihtiyaçların mevcut JSON-LD standart tanımlarının içerisinde bulunmadığı tespit edilmiştir. Blockcerts'in Türkiye'de uyumlu çalışabilmesi için JSON-LD üzerinde ek ihtiyaç alanlarının tanımlanabiliyor olması ihtiyacı ortaya çıkmıştır. Yapılan çalışmalar ve uygulama üzerinde yapılan ek geliştirmeler ile ihtiyaç duyulan niteliklerin ilgili JSON dijital diploma içerisinde tanımlandığı ve bu şekilde Bitcoin blokzincir ağı üzerinden uluslararası uyumlu diploma doğrulama yapılabildiği gözlenmiştir. Türkiye standartlarına uygun Blockcerts'e ek nitelikler tanımlanarak diploma üretilebildiği ve doğrulanabildiği görülmüştür. Böylelikle blokzincir teknolojisinin getirmiş olduğu kalıcılık ve güven ile birlikte Türkiye standartlarına uyumlu bir doğrulama metodunun gerçekleştirilmesi sağlanmıştır. Ek olarak çalışma kapsamında Türkiye'deki İstanbul Şehir Üniversitesi bünyesinde dijital diploma oluşturma, yayınlama, paylaşma ve doğrulama adımlarının uyum çalışması gerçekleştirilmiş ve bir yöntem ortaya konmuştur. Gerçekleştirilen çalışma detayları bu bölümde açıklanmıştır.

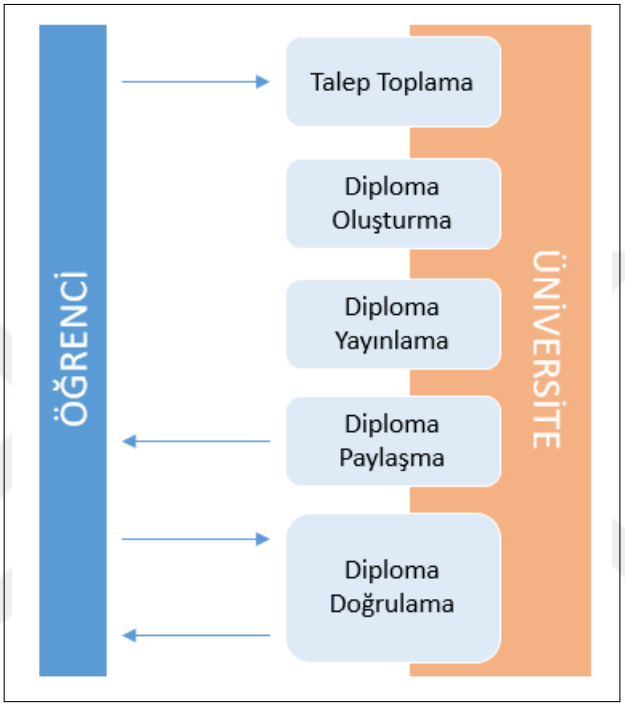
6.1 Gereksinim Analizi

Üniversite bünyesinde mevcut yapıyla bütünleşik çalışabilecek hafif ve esnek yapıya sahip bir çalışma kapsamında oluşturulacak blokzincir tabanlı diploma doğrulama yönetimi uygulama gereksinimleri aşağıdaki şekilde tespit edilmiştir.

- Kurum Cüzdanı (Açık Adres / Özel Anahtar): Dijital diplomanın kim tarafından üretildiği doğrulama aşamasında kritik rol almaktadır. Kurumun blokzincir üzerinde kendini temsil eden bir cüzdana sahip olması gerekmektedir. Yapılacak her yayınlama sürecinde kullanılmak üzere üniversiteye özel bir cüzdan oluşturulmalıdır.
- Erişim Sayfası: Üniversitenin bünyesin bulundurduğu geleneksel diploma yönetim sistemleri gibi uygulamalar ile bütünleşik blokzincir doğrulama sisteminin öğrenciler ile kullanıma girebilmesi için üç erişim sayfası bulunmalıdır.
  - Talebi Toplama: Üniversite öğrencisinden talebin alındığı bir ekran mevcut geleneksel öğrenci iletişim kanallarında yer alması,
  - İndirme: Toplanan talepler sonrasında öğrencinin, oluşturulan ve blokzincir üzerinde yayınlanan dijital diplomasının üniversite portalı üzerinden indirilmesine olanak tanıyan ara yüzün geliştirilmesi,
  - Doğruma: Gerek farklı kurumlarda, gerek üniversite tarafından üretilen dijital diplomaların doğrulanmasının kurum bünyesinde de yapılabilmesi için herkese açık bir sayfanın tasarlanıp, geliştirilmesi gerekmektedir.
- Uygulama Sunucusu: Uluslararası formata uygun dijital diploma üretiminin yapılacağı ve sonrasında blok zincir üzerinden doğrulanması için yayınlama sürecinin işletileceği bir uygulama sunucusuna,
- Uygulama Database: Üniversite öğrencilerinden toplanacak taleplerin takibi ve üretilen dijital diplomalar ile ilişkisinin tutulduğu bir veri tabanına,
- Rest API Servis Fonksiyonu: Üniversite bünyesindeki uygulamalar ile entegrasyonun ortak bir dil üzerinden sağlanabilmesi ve süreç yönetiminin basitleştirilmesi için geliştirilmesi gereken ek fonksiyonlara gereksinim vardır.

6.2 Süreç Analizi

Çalışma kapsamında üniversite bünyesinde oluşturulacak blokzincir tabanlı diploma yönetimi için belirli süreçlerin tespit edilmesi gerekmektedir. Öğrencinin talebini gerçekleştirmek adına üniversiteye dijital diploma oluşturma, yayınlama, paylaşma ve güvenli doğrulama mekanizmasının kazandırılması için belirli süreçlere ihtiyaç duyulmaktadır.



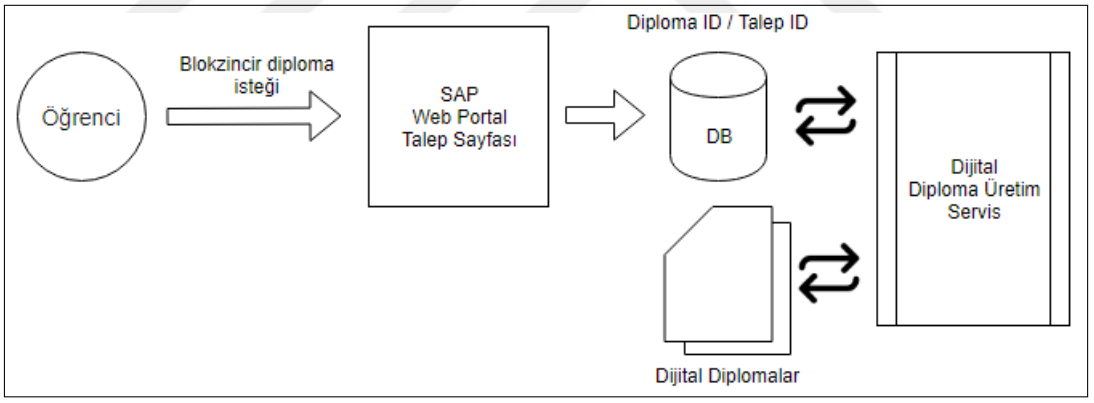
Şekil 6.1: Süreçler

- Talep toplama süreci: Talep bazlı gerçekleştirilmesi planlanan blokzincir diploma yönetiminde üniversite bünyesinde hangi öğrencinin, ne koşulda talep üretebildiğinin tanımını içeren ve taleplerin toplandığı süreçtir.
- Dijital, standart yapıda diplomayı oluşturma süreci: Diploma verilerinin kontrolünün sağlandığı, diploma tasarımının neler içereceğinin belirlendiği, kurum kimlik bilgilerinin doğruluğunun kontrolü ve oluşturulan dijital diplomanın hangi sunucuda ne şekilde saklanması gerektiği belirlenerek bu diploma oluşturulmaktadır.
- Dijital diplomanın özetini blokzincir ağına kaydetme, yayınlama: Ne kadar miktarda diplomaların özet değerinin blokzincir üzerinde kayıt altına alındığının tanımını içeren ve gerekli yayınlama işleminin gerçekleştiği süreçtir.

- İmzalanmış diplomayı öğrenci ile paylaşma: Yetki değerlendirmesinin yapıldığı ve dijital diplomanın yetkinlik sahibi ile paylaşıldığı süreçtir.
- Diploma doğrulama: Kurum bünyesinde blokzincir üzerinde yayınlanan diplomaların gerekli doğrulama kontrollerinden geçirerek, son kullanıcıya sonuç bilgisinin dönüldüğü süreçtir.

6.3 Talep Toplama ve Diploma Oluşturma

Çalışma kapsamında üniversite bünyesinde oluşturulacak blokzincir tabanlı diploma yönetimi yapısı için gerekli olan ilk adım diplomanın uluslararası formatta dijitalleştirilmesidir. Bu kapsamda kurum bünyesinde kullanılmakta olan SAP tabanlı öğrenci portalı üzerinden öğrencinin dijital diploma talebinin alınması ile süreç başlatılmaktadır. Alınan talep ile öğrencinin diploma bilgileri uygulama sucusuna aktarılarak dijital diplomasının bu bilgiler ışığında oluşturulması sağlanmaktadır. Oluşturulan dijital diploma JSON formatta sunucu üzerinde blok zincirde yayınlamak üzere kayıt altına alınmaktadır.



Şekil 6.2: Dijital Diploma Oluşturma Şeması

Bu süreç üzerine geliştirilen REST web servis fonksiyonları aracılığıyla diploma bilgileri JSON formatta SAP sunucusu üzerinden uygulamaya iletilerek SQLite veri tabanına kayıt edilmektedir. İçerisinde öğrenci bilgileri ve başarıyla mezun olduğu bölüm ve seviye bilgileri gibi gerekli bilgiler yer almaktadır. Periyodik olarak çalışan bir servis ile bu kayıt altına alınan yeni talepleri işleyerek daha önce konfigürasyon tabanlı oluşturulan dijital diploma tasarım şablonu ile yeni imzalanmamış diplomaları üretmektedir. Üretilen bu dosyaların bilgileri talep veri tabanına anlık olarak işlenmekte ve süreç takip altına alınmaktadır.

Tablo 6.1: Talep Toplama Yalancı Kod

```
Eğer öğrenci yeterlilik kazandıysa talep ekranını aktif et;
Öğrenciden talebi al;
Öğrencinin diploma bilgilerini çek;
Diploma bilgilerini formatla;
Diploma bilgilerini uygulama sunucusuna gönder.
```

Tablo 6.2: Dijital Diploma Oluşturma Yalancı Kod

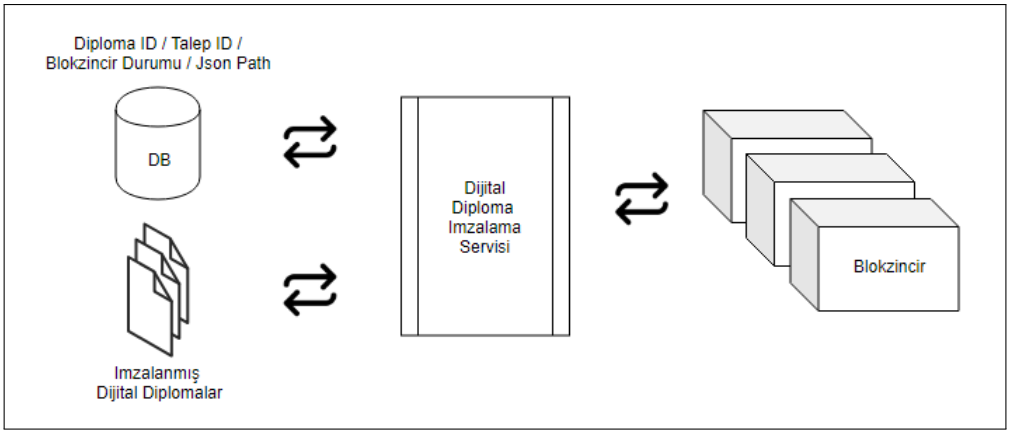
```
Yeni talebi veri tabanına durum 0 olarak kayıt et

Durum 0 olan talepleri her 5 dakikada bir tespit et;
Dijital diploma tasarımını oku;
Tespit edilen listeyi tek tek işle;
Dijital diplomayı tasarıma göre oluştur;
Dijital diplomayı dosya sistemine kayıt et;
Diploma dosya yolunu ve durumunu set et;
```

6.4 Diploma Yayınlama Tasarımı

Üretilen dijital diplomaların blokzincir üzerinden doğrulamasının yapılabilmesi için yayınlama adımının başarıyla işleme alınması gerekmektedir. Çalışma kapsamında talep ile dijitalleştirilen fakat daha henüz blokzincir üzerinde yayınlanmamış dijital diplomalar talep veri tabanında "unsigned" konumda barındırılmaktadır.

Tablo 6.3: Yayınlama Yalancı Kod

```
Yayınlayan kurum kimlik bilgileri temin et;
Yayınlanacak blokzincir bilgilerini temin et;
Geçici işlem klasörünü boşalt;
İmzalanmamış diplomaları tespit et;
İmzalanmamış dijital diplomaları geçici klasöre kopyala;
Geçici klasörde yer alan diplomaları imzala;
İmzalı diplomaları blokzincirde yayınla;
Yayınlanan diploma veri tabanı kayıtlarını güncelle;
```



Şekil 6.3: Dijital Diploma Yayınlama Şeması

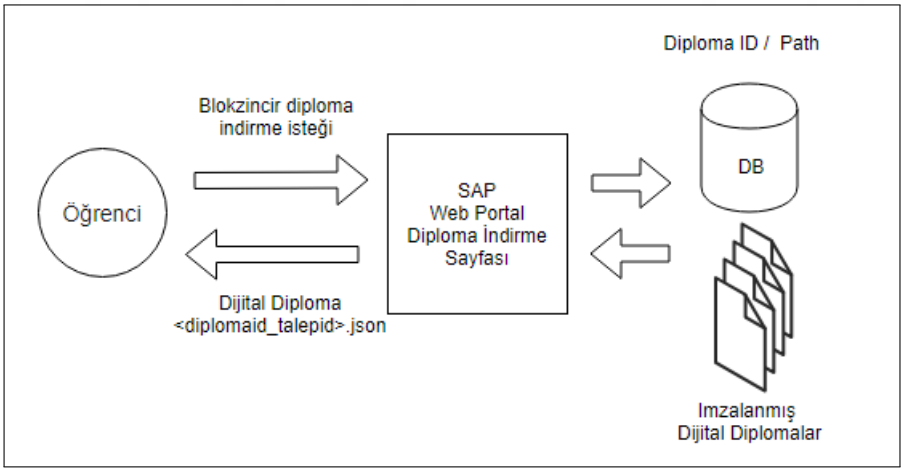
Çalışma kapsamında iki farklı yöntem ile yayınlama süreci işleme alınmıştır. Bunlardan bir tanesi anlık olarak mevcuttaki taleplerin eritilip saat fark etmeksizin blokzincir üzerinde yayına alınması sürecidir. Bir diğeri ise BackgroundScheduler kütüphanesi kullanılarak belirli tarihte çalışacak şekilde tanım yapılabilmektedir. Bu tetiklemeler sonrasında imzalanmamış dijital diplomalar tespit edilerek, grup halinde tek bir Bitcoin işlemi içerisinde yayınlaması yapılmaktadır. Yayınlama sonrasında elde edilen dosya yolu, işlem kimlik bilgileri SQLite veri tabanında paylaşım sürecinde kullanılmak üzere tutulmaktadır.

6.5 Paylaşım Süreç Tasarımı

SQlite veri tabanında tutulan dijital diploma talep bilgileri SAP portalı üzerinde geliştirilen paylaşım ekranı aracılığıyla öğrencilerin indirimine sunulmaktadır.

TABLO 6.4: Paylaşım Yalancı Kod

```
Paylaşılacak öğrenci diplomasını tespit et;
Blokzincir uygulamasından ilgili diplomaya ait verileri talep et;
Blokzincir uygulamasından imzalanmış diploma içeriğini talep et;
Talep edilen dijital diplomayı öğrenci ile paylaş
```

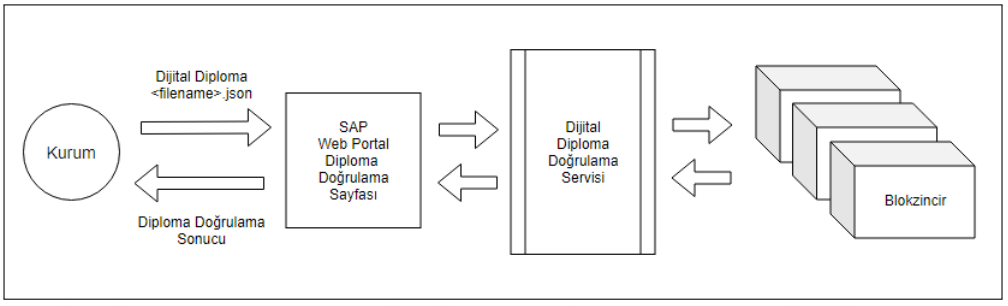


ŞEKIL 6.4: Dijital Diploma Paylaşım Şeması

6.6 Doğrulama Süreç Tasarımı

Doğrulama işlemi farklı web sayfaları üzerinden yapılabildiği gibi aynı zamanda üniversite bünyesinde de bu süreç tasarlanmıştır. Kuruma gelen standartlara uygun JSON

dosyası herkese açık bir sayfa üzerinden güvenlik kontrolleri uygulanarak incelenmektedir. Bu kontroller dosya boyutu, dosya tipi ve içerik taraması olarak belirlenmiştir. Kontrollerden geçen dosya doğrulama sürecine tabi tutulmaktadır. Cert-Verifier python modülü kullanılarak gerçekleştirilen doğrulama adımlarının sonucu istemciye uygun bir tasarım ile sunulmaktadır.



Şekil 6.5: Dijital Diploma Doğrulama Şeması

6.7 Diploma Tasarımı

Oluşturulan JSON formattaki dijital diplomanın görselleştirilmesi Blockcerts içeriğindeki Viewer kütüphanesinde varsayılan olarak yapılmaktadır. Fakat kurumlar daima kendi tasarımlarını kullanmayı tercih etmektedirler. Bu sebeple bu görselleştirme alanının kişiselleştirilebiliyor olması tercih edilen bir özellik olmuştur. Diplomanın özel görselleştirilmesi için JSON dosya içerisinde "displayHtml" alanı kullanılmalıdır. Bu alanda html etiketler kullanarak kuruma özel tasarımlar ortaya konabilmektedir. Çalışma sonunda İstanbul Şehir Üniversitesi için tasarlanan şablon ile test Bitcoin blokzincirinde yayınlanmış örnek bir diplomayı ŞEKİL 6.6'da görebilirsiniz.

Şekil 6.6: Blokzincir Üzerinde Yayınlanmış Diploma Örneği

6.8 Entegrasyon Efor Analizi

Gerçekleştirilen örnek çalışma sırasında kullanılan teknolojiler ve kütüphaneler minimal seçilerek iş, harcanan efor ve kaynak tüketim maliyetleri düşürülmüştür. TABLO 6.5'de de gösterildiği üzere, ilgili ürünlerde tecrübe sahibi olmayan geliştiricilerin benzer bir çalışmayı ortaya koyabilmesi için gerekli bilgi düzeyi Başlangıç, Orta ve İyi şeklinde sınıflandırılarak değerlendirmeye tabi tutulmuştur. Çalışma sırasında elde edilen çıktılar değerlendirilerek bilgi edinme süresi ile geliştirme süreci için adam/gün maliyet hesaplaması ortaya konmuştur.

Tablo 6.5: Kullanılan Ürünlerin Gelişme Maliyet Tablosu

Ürün	Kısa Açıklama	Bilgi Seviyesi	A/G
Ubuntu	İşletim Sistemin	Başlangıç	1
Python3	Programlama Dili	Orta	3
PyCharm	Geliştirme Platformu	Başlangıç	1
Apache	Web Server	Başlangıç	1
WSGI	Web Sunucu Ağ Geçidi Arayüzü	Başlangıç	1
Flask	Minimal Web Python Kütüphanesi	Orta	4
SQLite3	Veri Tabanı	Orta	2
BlockCerts	Açık Kaynak MIT Kütüphanesi	İyi	3

Kurum bünyesinde kullanılan SAP gibi teknoloji ve tecrübe birikimleri değerlendirmeye alınmamıştır. Farklı kurumlarda mevcut bir yapının kurulması sırasında teknolojik birikimin elde edilmesi ve geliştirmenin sağlanması için yaklaşık 16 adam gün maliyet ortaya çıkmaktadır.

Bölüm 7

Sonuç

Yetkinlik doğrulama süreci günümüzün problemi olup birçok kamu ve özel kuruluşlarda mağduriyetlere ve haksız kazançlara sebebiyet vermektedir. Mevcut süreçlerdeki dağınıklık ve mahalli çözümler, problemi genel manasıyla çözmemektedir. Uygulanan çözümlerde günümüz saldırılarına açık olup bütünlük açısından sorun teşkil etmektedir. Merkezi çözümler tek bir nokta da oluşabilecek bir manipülasyona daima açıktır ve ona bağlı olan güveni de beraberinde yıkmaktadır. Dünyada ortaya konulan çözümlerin incelenmesi ile beraber bünyesinde birden fazla çözümü barındıran bir yaklaşım olan blokzincir yaklaşımı güvenilirliği ile ön plana çıkmaktadır. Yapısının derinlemesine incelenmesi akabinde mevcut yaklaşımlar ile karşılaştırıldığında blokzincir yaklaşımının doğrulama alanında ihtiyaç duyulan güvene farklı bir boyut kattığı gözükmektedir. Kullandığı mimari ve güven inşası için oluşturduğu metotlar, katmanlar halinde inceleme ile benzersiz, merkezsiz güvenilir bir yapı olduğu ortaya konmaktadır.

Değerli evrakların doğrulamasının güvenilir olması için kullanılan teknoloji kadar şeffaflık, kullanılabilirlik, süreç ve uyum gibi kavramlarda önemlidir. Diploma doğrulama yöntemi güvenilir olması ve beraberinde geniş alanda etkin bir çözüm olabilmesi için gerekli olan şeffaflık, kullanılabilirlik, süreç ve standartlara uyum kavramları ile değerlendirmeye alındığında gerçekleştirilen çalışmayla beraber Blockcerts çözümünün ek geliştirmeler ile ihtiyaçları karşıladığı ortaya koyulmuştur. Özellikle Türkiye'deki diplomalar için gerekli alanların aynı çözüm ile uygulanabiliyor olduğu gösterilmektedir.

Böylelikle MIT gibi farklı ülkelerdeki kuruluşlar ile ortak bir çözüm olduğu belirtilmektedir. Birçok doğrulama adımının incelenmesi ve ilişkilerinin ortaya konması ile belirsizlik ortadan kaldırmaktadır.

İstanbul Şehir Üniversitesi bünyesine blokzincir tabanlı diploma yönetim uygulamasının geliştirmesi ve entegrasyonu kapsamında birçok konu ele alınmaktadır. Diploma doğrulama yönetimi için gerekli oluşturma, yayınlama, paylaşma ve doğrulama süreçlerinin çıkartılması ve detaylandırılması yapının kullanılabilirliğine örnek olarak sunulmuştur. Avantajları ve riskleri ile ortaya konan blokzincir tabanlı Blockcerts uygulama çalışması ile çözümün ortaya çıkarttığı gereksinimler ve maliyetler belirtilmiştir. Ortaya konan çözüm, geliştirme ve metot önerileri ile beraber diploma doğrulama çözümlerindeki problemlerin ortadan kaldırılması hedeflenmektedir. Böylelikle yaşanacak haksız kazanımların ve mağduriyetlerin önüne geçilmesi hedeflenmektedir. Lokal bir çözüm yerine her yönüyle güvenilir uluslararası bir çözümün tercih edilmesi gerektiği aktarılmaya çalışılmıştır.

Kaynaklar

[1] S. Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Diplomamakers. Welcome to diploma makers, March 2018. URL https://diplomamakers.com.

[3] Yeniakit. Meb'de sahte diploma skandalı, March 2018. URL https://www.yeniakit.com.tr/haber/mebde-sahte-diploma-skandali-tam-153-ogretmen-278943.html.

[4] Cnnturk. Avcılar'da sahte belge operasyonu, May 2019. URL https://www.cnnturk.com/video/turkiye/avcilarda-sahte-belge-operasyonu.

[5] G. Grolleau, T. Lakhal, and N. Mzoughi. An introduction to the economics of fake degrees. *Journal of Economic Issues*, 2008.

[6] T24. Tubitak'ta ikinci sahte diploma skandalı, April 2015. URL https://t24.com.tr/haber/tubitakta-sahte-diploma-skandali,284377.

[7] EDevlet. Yukseogretim mezun belgesi sorgulama, April 2018. URL https://www.turkiye.gov.tr/yuksekogretim-mezun-belgesi-sorgulama.

[8] Haber7. E-devlet'e erişimde sorun., April 2018. URL http://www.haber7.com/teknoloji/haber/2401171-e-devlete-erisimde-sorun-btkdan-aciklama-geldi.

[9] MIT. Degree verification, April 2018. URL https://credentials.mit.edu/.

[10] OS University. The world's academic career development ledger, April 2018. URL https://os.university/.

[11] Melbourne University. Melbourne university to pilot a distributed database for micro-credentials, April 2018. URL http://newsroom.melbourne.edu/news/melbourne-university-pilot-distributed-database-micro-credentials-0.

[12] Blockcerts. Universal verifier, March 2018. URL https://www.blockcerts.org/.

[13] YÖK. Yükseköğretim mevzuatları, April 2018. URL https://www.yok.gov.tr/kurumsal/mevzuat.

[14] Mevzuat. Yükseköğretim kanunu, March 2018. URL http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2547.pdf. Madde 43.

[15] G. Aelterman, B. Curvale, A. Erdogan, E. Helle, S. Karki, C. Miles, and F. Profit. Study on the diploma supplement as seen by its users, 2008.

[16] Enic-Naric. The diploma supplement, April 2018. URL https://www.enic-naric.net/fileusers/THE_DIPLOMA_SUPPLEMENT.pdf.

[17] İstanbul Üniversitesi. Diploma eki, April 2018. URL http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=diploma_eki.pdf.

[18] IMS Global Learning Consortium. Open badges v2.0 ims final release, March 2018. URL https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/index.html.

[19] Blockcerts. Blockcerts standards alignment, March 2018. URL https://www.blockcerts.org/guide/standard.html.

[20] M. Taşçıoğlu, C. Yıldız, and D. E. Aydın. Üniversite diplomalarının tasarlanması. page 93, 2018.

[21] Haberturk. Bin liraya diploma, April 2018. URL http://www.haberturk.com/yasam/haber/586991-bin-liraya-diploma.

[22] University Of Oxford. Verifying qualifications, May 2018. URL https://www.ox.ac.uk/students/graduation/verification?wssl=1.

[23] University Of Cambridge. Verification of degrees, May 2018. URL https://www.cambridgestudents.cam.ac.uk/your-course/graduation-and-what-next/verification-cambridge-degrees.

[24] Sakarya Üniversitesi. Diploma dogrulama sistemi, May 2018. URL http://www.ogrisl.sakarya.edu.tr/tr/icerik/9804/34476/diploma-sorgulama.

[25] Qualificationcheck. Qualificationcheck fast, secure education verifications, May 2018. URL https://www.qualificationcheck.com.

[26] Edx. Earn your edx verified certificate and share it with the world., April 2018. URL https://www.edx.org/verified-certificate.

[27] E-Devlet. E-devlet barkodlu belge dogrulama, March 2018. URL https://play.google.com/store/apps/details?id=tr.gov.turkiye.belgedogrulama&hl=tr.

[28] Sony. Sony global education creating a trusted experience with blockchain, April 2018. URL https://blockchain.sonyged.com/.

[29] CoinFirm. Coinfirm amlt, the token of compliance, May 2018. URL https://www.trudatum.com/pdf/white-paper.pdf.

[30] Gradbase. Gradbase limited. let's end cv fraud. for good, March 2018. URL https://gradba.se.

[31] S. Das. Melbourne university to pilot blockchain for student records in aussie-first, May 2018. URL https://www.ccn.com/melbourne-university-pilot-blockchain-student-records-aussie-first/.

[32] Bestr. Bestr becomes a digital credentials ecosystem, December 2018. URL https://blog.bestr.it/en/2018/10/15/blockchain-and-open-badges-bestr-becomes-digital-credentials-ecosystem.

[33] SNHU. Blockchain pilot empowers ownership, access of school records, May 2018. URL https://www.snhu.edu/about-us/newsroom/2018/06/blockchain-securing-school-records.

[34] Blockcerts. Issuing prerequisites, March 2018. URL https://github.com/blockchain-certificates/cert-issuer/.

[35] D. Xiao. The four layers of the blockchain, June 2018. URL https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f.

[36] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. 2012.

[37] V. Buterin. Etherium. proof of stake faq. June 2018. URL https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

[38] P4Titan. A peer-to-peer crypto-currency with proof-of-burn. June 2018. URL `https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf`.

[39] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak. Proofs of space. May 2018. URL `https://eprint.iacr.org/2013/796.pdf`.

[40] A. Back and Others. Hashcash-a denial of service counter-measure. 2002.

[41] H. Gilbert and H. Handschuh. Security analysis of sha-256 and sisters. In *International workshop on selected areas in cryptography*, pages 175–193. Springer, 2003.

[42] D. Vujičić, D. Jagodić, and S. Ranđić. Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pages 1–6. IEEE, 2018.

[43] Bitcoin. Bitcoin block height and forking, March 2018. URL `https://bitcoin.org/en/blockchain-guide#block-height-and-forking`.

[44] R. C. Merkle. Protocols for public key cryptosystems. In *1980 IEEE Symposium on Security and Privacy*, pages 122–122. IEEE, 1980.

[45] Bitcoin. Github repository, March 2018. URL `https://github.com/bitcoin/bitcoin`.

[46] Ethereum. Github repository, March 2018. URL `https://github.com/ethereum/`.

[47] R. Matzutt, J. Hiller, M. Henze, J. H. Ziegeldorf, D. Müllmann, O. Hohlfeld, and K. Wehrle. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer*, 2018.

[48] Bernstein. Intellectual property for the digital age, May 2018. URL `https://www.bernstein.io`.

[49] Bitcoin. Technical background of version 1 bitcoin addresses, June 2018. URL `https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses`.

[50] D. Massessi. Public vs private blockchain in a nutshell, June 2018. URL https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f.

[51] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox. Zcash protocol specification. *Tech. rep. 2016–1.10. Zerocoin Electric Coin Company, Tech. Rep.*, 2016.

[52] Blockcerts. Blockcerts wallet, June 2018. URL https://play.google.com/store/apps/details?id=com.learningmachine.android.app&hl=en.

[53] İstanbul Şehir Üniversitesi. Önlisans ve lisans eğitim-öğretim ve sınav yönetmeliği. June 2018. URL https://www.sehir.edu.tr/tr/Documents/Yonetmelikler/IstanbulSehirUniversitesiOnlisansLisansEgitimOgretimSinavYonetmeligi.20170219.pdf.

[54] Sakarya Üniversitesi. Diploma mezuniyet belgesi İle diğer belgelerin düzenlenmesinde uyulacak esaslara ilişkin yönerge. June 2018. URL http://www.ogrisl.sakarya.edu.tr/tr/icerik/8852/31931/diploma-yonergesi.

[55] Uludağ Üniversitesi. Önlisans ve lisans öğretim yönetmeliği. August 2018. URL http://www.uludag.edu.tr/dosyalar/ysehirmyo/duyuru_dosyalar/y%C3%B6netmelik%2012.01.2017.pdf.

[56] Akdeniz Üniversitesi. Mezuniyet ve mezuniyet belgeleri yönergesi. August 2018. URL http://yazi.akdeniz.edu.tr/wp-content/uploads/2016/10/12temmuzx.doc.

[57] Süleyman Demirel Üniversitesi. Mezunlara verilecek belgelerin düzenlemesine ilişkin yönerge. August 2018. URL https://oidb.sdu.edu.tr/assets/uploads/sites/73/files/mezunlara-verilecek-belgelerin-duzenlemesine-iliskin-yonerge.docx.

[58] Eskişehir Osmangazi Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://oidb.ogu.edu.tr/Sayfa/Index/125.

[59] Ankara Yıldırım Beyazı Üniversitesi. Diploma yönergesi. August 2018. URL https://kms.kaysis.gov.tr/Home/Goster/74014?AspxAutoDetectCookieSupport=.

[60] Karadeniz Teknik Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://www.ktu.edu.tr/dosyalar/oidb_32f04.pdf.

[61] Anadolu Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL https://www.anadolu.edu.tr/uploads/anadolu/files/bilgi-ve-belge/576a6f2c9fa10.pdf.

[62] Bursa Teknik Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://depo.btu.edu.tr/img/senatokarar_dosyalar/1448368784_Bt%C3%BC%20Diploma,%20Diploma%20Eki%20%C4%B0le%20Di%C4%9Fer%20Belgelerin%20D%C3%BCzenlemesine%20ili%C5%9Fkin%20Y%C3%B6nerge.pdf.

[63] İstanbul Zaim Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://www.izu.edu.tr/ogrenci/kayit-kabul/yonerge-yonetmelikler/yonergeler/diploma-sertifika-ve-di%C4%9Fer-i-lgili-belgelerin-d%C3%BCzenlenmesine-i-li%C5%9Fkin-y%C3%B6nerge.

[64] Dokuz Eylül Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://ogrenci.deu.edu.tr/index.php?option=com_content&view=article&id=19&Itemid=145&lang=tr.

[65] Bezm-İ Alem Vakif Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://ns2.bezmialem.edu.tr/docs/Diploma-ve-diger-ilgili-belgelerin-duzenlenmesine-iliskin-yonerge.pdf.

[66] Atatürk Üniversitesi. Diploma, mezuniyet ve diğer belgelerin düzenlenmesi ile ilgili uygulama esaslari. August 2018. URL http://www.atauni.edu.tr/yuklemeler/c23e051bbca11cfc701c21bbe058d74e.doc.

[67] Ege Üniversitesi. Diploma, diploma eki ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://fenbilimleri.ege.edu.tr/wp-content/uploads/2014/04/diploma-Y%C3%B6nergesi-yeni-hali.pdf.

[68] Gebze Teknik Üniversitesi. Mezuniyet belgeleri ile diploma ve diploma defterinin düzenlenmesinde uygulanacak esaslara ilişkin yönerge. August 2018. URL

http://www.gtu.edu.tr/Files/UserFiles/130/YO-006_Mezuniyet_Belgeleri_Ile_Diploma_ve_Diploma_Defterinin_Duzenlenmesinde_Uygulanacak_Esaslara_Iliskin_Yonerge.doc.

[69] Ankara Üniversitesi. Diploma yönergesi. August 2018. URL http://oidb.ankara.edu.tr/files/2015/01/diplomayonerge.pdf.

[70] İstanbul Üniversitesi. Mezuniyet belgeleri ile diploma ve diploma defterlerinin düzenlenmesinde uyulacak esaslara ilişkin yönerge. August 2018. URL http://www3.istanbul.edu.tr/oidb/mevzuatdosyalar/Yonergeler/Diploma_Yonergesi.html.

[71] İstanbul Teknik Üniversitesi. Mezuniyet belgeleri ile diploma ve diploma defterleri, sertifika ile diğer belgelerin düzenlenmesinde uyulacak esaslara ilişkin yönerge. August 2018. URL http://www.sis.itu.edu.tr/tr/yonetmelik/Diploma.html.

[72] Hacettepe Üniversitesi. Diploma, sertifika, geçici mezuniyet ve diğer belgelerin düzenlenmesine ilişkin yönerge. August 2018. URL http://www.hacettepe.edu.tr/duyuru/yonergeler/51,snyk231110yeni.pdf.

[73] Ardahan Üniversitesi. Diploma eki. January 2018. URL www.ardahan.edu.tr/dosyalar/icerik/oidb/yonerge/DiplomaEkiNedir.pdf/.