©2018 Published in 6th International Symposium on Innovative Technologies in Engineering and Science 09-11 November 2018 (ISITES2018 Alanya – Antalya - Turkey)

Türkiye ve Avrupa Birliği Standartlarına Uygun Blokzincir Tabanlı Diploma Paylaşma ve Doğrulama Çözümü

Ekrem Yasir İKİZOĞLU
İstanbul Şehir Üniversitesi, Bilgi Güvenliği Mühendisliği, İstanbul Türkiye
Oktay ADALIER
TÜBİTAK BİLGEM UEKAE Kocaeli, Türkiye
Ensar GÜL
İstanbul Şehir Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul Türkiye

Abstract
Organisation's stamp or wet signature are 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, make documents like the original and very difficult to undersatand the fake ones. Because of such fraud many private and public institutions are emploing unqualified and unreliable employees or rights holders are victims of such situations. Approved very important documents informations such as the validity, the accuracy, when and by whom it given should not be easily reached. In this study, the scope of the creation and validation of valuable documents was defined by defining its processes. Also, examples in the World and the degree (diploma) management dimension in Turkey were discussed. Data structures in accordance with the standards and apllied regulations in our country have been researched and requirements have been determined. Blockcerts solution working on blockchain architecture has been chosen according to the determined needs. Thus, using an accepted architecture according to Turkey's standard of diploma verification structure made to move to an international position. As a result, classical solution methods in Turkey were compared with equivalents made in the World.

Özet
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 çalıştırmakta veya hak sahipleri bu gibi durumlardan mağdur olmaktadır. Değeri yüksek, bir kurum tarafından onaylanmış belgelerin doğruluğu, geçerliliği ve kimin tarafından ne zaman verildiği gibi bilgiler kolay bir şekilde netliğe kavuşturulamamaktadır. Bu çalışmada değerli belgelerin oluşturulması ve doğrulaması işlemlerinin tanımı yapılarak, kapsamı belirlenmiştir. 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. Böylelikle kabul görmüş bir mimariyi kullanarak Türkiye'nin standartlarına uygun diploma doğrulama yapısını uluslararası bir konuma taşıması yapılmıştır. Sonuç olarak yapılan çalışma Türkiye'deki klasik çözüm metodu ve dünyadaki yapılan muadilleri ile karşılaştırılmıştır.

Anahtar Kelimeler— blokzincir, eğitim, diploma, doğrulama

*Sorumlu Yazar: İstanbul Şehir Üniversitesi, Bilgi Güvenliği Mühendisliği, İstanbul Türkiye

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 kâğıt 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 [1]. Yakın tarihimizde üniversitelerde, özel kurumlarda ve ülke için kritik pozisyonda bulunan firmalarda sahte diploma vakaları meydana gelmiştir [2]. 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 [3].

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 [4]. Fakat geleneksel merkezi veri tabanları üzerine kurulan bunun gibi yapılar mevcut verinin değiştirilmesi, bozulması veya erişimin kesilmesi gibi problemler barındırmaktadır [5]. Bu sebepten daha güvenilir, hızlı ve kolay doğrulama yapabileceğimiz bir çözüme ihtiyaç bulunmaktadır.

Diploma, sertifika gibi değerli dokümanların hızlı, güvenilir bir yöntemle doğrulanması için blokzincir tabanlı çözümler geliştirilmiştir [6,7,8]. 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'deki çözümler ile uluslararası bir çözümün karşılaştırılması yapılmıştır. Türkiye'deki üniversitelerde diploma oluşturulmasında uygulanan standartlar ile Blockcerts sertifika yapısının ilişkilendirilmesi yapılmış, ihtiyaçların tespiti sonrası gerekli ek çözümler sunulmuştur [9]. Kabul görmüş bir yapıyı kullanmak ve Türkiye'nin standartlarına uygun diploma doğrulama yapısını uluslararası bir konuma taşıma çalışması gerçekleştirilmiştir.

2. İlişkili Çalışmalar

Bu bölümde diploma gerekliliklerine ve doğrulama süreci için geliştirilmiş mevcut çözümlere değinilmiştir. Mevcut çözümlerin ele alınması sonrasında Türkiye'nin mevcut yapısı ile diğer metotların güvenlik kapsamında karşılaştırılmasını yapılmıştır. Karşılaştırma neticesinde seçtiğimiz Blockcerts çözümünün altyapısı olan blokzincir teknolojisinin tarihi, mimarisi, kayıt edilebilen veri türleri ve blokzincir ağ türleri konularından bahsedilmiştir.

2.1. Diploma Gereklilikleri

Bir okul veya öğrenim programının başarıyla tamamlandığını gösteren diplomalar belli başlı özellikleri bünyesinde barındırmalıdır [10,11]. Bilgilendirici; sağlanan başarının ne ifade ettiği, hangi konuda başarı sağlandığı gibi gerekli bilgileri içermelidir. İptal Edilebilir; verilen diplomalar belli bir nedenden dolayı iptal edilebilmelidir. Paylaşılabilir; diplomayı almaya hak kazanan kişiler belgelerini dilediği gibi paylaşabilmelidir. Doğrulanabilir; diplomaların doğrulanması herkesçe yapılabilmelidir. Diplomanın

değişikliğe uğramadığını çözümlemek için kullanılan metodunda iyi tasarlanmış ve kolay uygulanabiliyor olması gerekmektedir. Veren-Alan; diploma içerisinde diplomayı veren ve alan kişi veya kurumların belirgin bir şekilde tanımlanıyor olması gerekmektedir. Standartlara uyumlu; oluşturulan diplomalar bulunduğu ülkenin veya bağlı olduğu kurum ve kuruluşların yayınladıkları yönetmeliklerinin koyduğu standartlara uyumlu olmalıdır.

Uyum Standartları: 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. YÖK yönetmeliğinde diploma üzerinde alan kişinin kayıtlı olduğu enstitü anabilim/anasanat dalındaki programın Yükseköğretim Kurulu tarafından onaylanmış adının bulunması gerektiği belirtilmiştir [11]. 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 [39,40,41]. Avrupa Komisyonu, Avrupa Konseyi ve UNESCO/CEPES tarafından belirlenen format ile Avrupa birliği tarafında kabul edilerek 22 ülke tarafından kullanılmaktadır [12]. Kazanılan başarının uluslararası yeterli düzeyde tanınmasını sağlayan diploma eki Türkiye'de de diploma ile beraber verilmektedir [15].

Open Badge: IMS Global Learning Consortium tarafından dijital ortamda hangi yetkinliğin kim tarafından kime verildiğinin doğrulanması amacıyla geliştirilen bir standarttır [16]. JSON-LD veri yapısını kullanıldığı bu standartta alıcı, verici kimliklerinin yapı içerisindeki bağlantılar ile doğrulanması sağlanmaktadır. Bu standart, blokzincir mimari yapısında işlemler gerçekleştiren Blockcerts çözümü içerisinde kullanılmaktadır [9].

2.2. Diploma Doğrulama Çözümleri

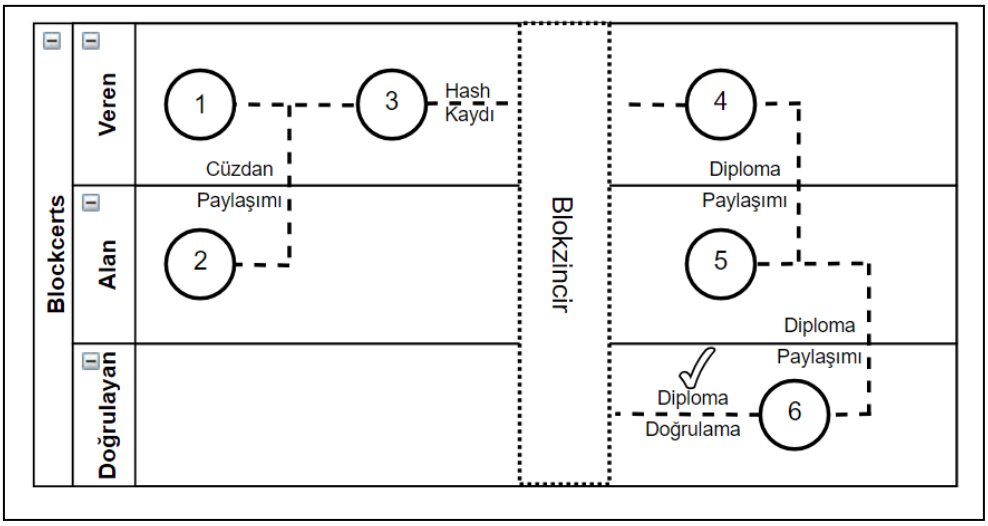
Diplomanın sahtesinin tespiti için günümüzde fiziki çözümlerin yanı sıra dijital ortam çözümleri geliştirilmiştir. Fiziki: Günümüzde diplomalar kâğıt baskı üzerinde verilmeye devam edilmektedir. Bu fiziki dokümanların taklidini önleyebilmek için her kurum kendi yönetmeliğinde yer alan çözümler ile önlemler almaktadır. Hologram, ıslak imza, özel tasarım şablonlar, kare kod veya kabartma gibi metotlar ile belgenin sahte olup olmadığının doğrulanması hedeflenmiştir. Fakat günümüz teknolojisinde kabartma, kare kod, hologram veya ıslak imzalar kolayca taklit edilebilmektedir [1,2,3,17].

Dijital Çözümler: Üniversiteler verdikleri belgelerin doğruluğunun yapılabilmesi için kendi web sayfalarına yönlendiren bağlantıları diploma üzerine işlemektedirler [18]. 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 [19]. Cambridge Üniversitesi kendi sayfasındaki yönlendirmelerinde bulunan mail adresi üzerinden doğrulama süreci sunmaktadır [20]. Sakarya Üniversitesi'nde ise diploma üzerindeki bağlantı üzerinden diploma numarası ile doğrulama yapmaktadır [9]. Üniversitelerin bu tür yaklaşımları 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. İşverenler için farklı üniversite ve kurumlar ile doğrulama yapma zorluğu sebebiyle Qualificationcheck, EdX gibi özel çözümler doğmuştur [21,22]. Farklı kurumların doğrulamasını tek çatı altından işverenlere sunulması fikrinden yola çıkarak farklı uluslardaki yükseköğretim kurumlar ile anlaşarak geliştirdikleri web servisler ile işverenlere yetkinlik doğrulama hizmeti satmaktadırlar. EdX üzerinden yetkinlik kazanan bireylerin sertifikaları kolaylıkla doğrulanabilir ve paylaşılabilir. Bu platformlarda üretilen diplomalar standart uyumluğu, kalıcılık problemleri içermekte ve merkezi bir yapıdan sunulmaktadır.

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 E-Devlet veri tabanlarına aktarması ile tek bir kanal üzerinden doğrulama yapılabilmektedir. E-Devlet üzerinden çıkartılan diplomanın üzerinde doğrulama bağlantısı bulunmaktadır. Bu bağlantı üzerinden E-Devlet sunucuları üzerinde doğrulama yapılabilmektedir [4]. Merkezi bir platformda sunulan bu yapı üzerinde yaşanacak problemler ve veriler üzerinde yapılacak izinsiz değişiklikler ile veri bütünlüğü ve kalıcılık problemleri söz konusu olabilmektedir.

Merkezi çözümlerin dışında merkezi olmayan bir yapı sunan blokzincir mimarisi kullanılarak üzerinde diploma doğrulama yapılabilen çözümler bulunmaktadır. Sony Global Education firmasının sunduğu eğitim programlarının sertifikalarını blokzincir mimarisi üzerinden doğrulama çözümü geliştirmişlerdir [23]. Global Math Challenge gibi programlarda kullanılmakta olan bu uygulama ile oluşturan sertifikaların PNG formatı üzerinden doğrulaması yapılabilmektedir. Coinfirm tarafından geliştirilen Trudatum çözümü ile dokümanların doğrulamasına olanak sağlamaktadır [24]. Doğrulamayı blokzincir üzerinden yapmakta ve her işlem için ücret almaktadır. Grandbase sayfasında her üç kişiden birinin CV'lerinde yalan söylediğini belirterek Bitcoin'nin blokzincir yapısı üzerinden beyan edilen yeteneklerin doğruluğunu kullanıcılarına sunmaktadır [25]. Bu çözümlerin standart uyumlulukları bulunmamakta ve doğrulama adımlarında kullandıkları yaklaşımların belirsiz olması sebebiyle güven problemi doğurabilmektedir. Bunların dışında MIT lisanslı açık kaynak kodlu bir proje olan Blockcerts çözümü JSON-LD formatındaki sertifikaların doğrulanması sürecini Bitcoin işlemleri yapısında bulunan alanları kullanılarak gerçekleştirmektedir. Diplomayı veren ve alanın doğru bir şekilde tanımlandığı ve onaylama adımlarının açık bir şekilde gözlemleyebildiğimiz bir yapı ortaya koymaktadır. Merkezi olmayan blokzincir yapılarını kullanan Blockcerts uygulamasında diploma yayınlama, paylaşma ve doğrulama adımları yapılabilmektedir. MIT Üniversitesi öğrencilerinin diplomalarını bu şekilde öğrencileri ile paylaşmakta ve doğruluğunu sağlamaktadır.

Resim 1. Blockcerts Akış Şeması



2.1. Metotları Karşılaştırması

Bir önceki bölümde bahsedilen diploma doğrulama hususundaki çözüm metotlarının farklı özellikler üzerinde karşılaştırması TABLO I'de yapılmıştır.

Tablo 1. Farklı çözümlerin Karşılaştırılması.

Metot	Özellikler					
	Doğrulana-bilirlik		*İptal Edile-bilirlik*	*Uyum-luluk*	*Kalıcı*	*Merkezsiz*
	Güven	*Hız*				
Üniversite	Orta	Kötü	Evet	Evet	Hayır	Hayır
E-Devlet	Orta	Orta	Evet	Evet	Hayır	Hayır
Qualification-check	Orta	Orta	Evet	Hayır	Hayır	Hayır
Grandbase	Orta	İyi	-	Hayır	Evet	Evet
Blockcerts	İyi	İyi	Evet	Kısmen	Evet	Evet

Karşılaştırma sonucunda uyumluluğa ek merkezsiz oluşu ve kalıcılığı sağlaması yönünden ve sunmuş olduğu şeffaflık sayesinde doğrulama mekanizması olarak Blockcerts kullanımı avantajlı gözükmektedir. Blockcerts gibi bir yapı üzerinden doğrulama işlemlerinin gerçekleştirilmesini daha iyi görebilmek için swot analizi üzerinde de incelenmiştir.

Güçlü:

- Maliyetler açısından verimlilik getirmesi
- Kolay entegrasyon/uyum sağlanabilmesi
- Herkesçe ve hızlı doğrulanabilir olması
- Tek arıza noktası buldurmayan merkezsiz bir yapı olması
- Güvenlik protokollerinin gelişmiş olması

Fırsatlar:

- Kalıcılığın üst seviyede olması
- Uluslararası bir çözüm sunması
- Güncel teknolojiyi yakalama fırsatı sunması

Tehditler:

- Çok fazla işlem, yük meydana gelebilmesi
- Saldırgan kişilere çok açık olması

Zayıf Yönler:

- Mevzuat ve bilgi yetersizliği
- Yeni kavramlar içermesi

Yapılan analiz gösteriyor ki blokzincir yapısına sahip merkezsiz mimariler evrak doğrulamasında önemli faydalar içermektedir. Fırsatlar ve güçlü yanları sebebiyle evrak yönetiminde kullanılması çok yararlı olacaktır.

2.2. Blokzincir

Bu bölümde Türkiye'deki doğrulama sürecinde kullanmayı önerdiğimiz Blockcerts'in kullandığı blokzincir teknolojisinden bahsedilmiştir.

2.4.1 Blokzincir Tarihi

Blokzincir ilk olarak 2008 yılındaki Satoshi Nakamoto takma adı altındaki makale ile sunulan Bitcoin uygulamasının altyapısı olarak tanımlanmış ve kullanımına 2009 yılında oluşturulan ilk blok ile başlanmıştır [26]. Blokzincir; içerisinde çeşitli tiplerdeki verilerin içeren blokların eklemeli olarak birbirine bağlanması ile oluşmakta ve dağıtık yapıda bulunan düğümler arasında paylaşılmaktadır.

2.4.2 Blokzincir Mimarisi

Bu bölümde blokzincir uygulamaları mimari açıdan konsensüs, madencilik, yayılım, doğrulama ve uygulama olmak üzere beş katman hakkında kısaca bahsedilecektir [28].

Konsensus Katmanı: Blokzincir oluşturan blokların format tanımlamalarının yapıldığı, yeni blokların oluşturulmasında ve doğrulanmasında farklı düğümler ile güvenin inşası için mutabakat protokolünün belirlendiği bölümü konsensüs katmanı olarak tanımlayabiliriz. [26]'deki Bitcoin uygulaması üzerinde Emek İspatı (Proof of Work) konsensüsü uygulanmaktadır. Bunun dışında Proof of Stake, Proof of Burn ve Proof of Space gibi çeşitli konsensüs yaklaşımları da geliştirilmiştir [29,30,31]. Emeğin ispatı yaklaşımında güvenin inşası için belirli bir emeğin ortaya konulması gerekmektedir. İlk kez Hashcash üzerinde kullanılan emeğin ispatı protokolü Bitcoin'de zaman ve işlem hacmi gerektiren SHA-256 özet alma fonksiyonu üzerinden işletilmektedir [26,32].

Madencilik Katmanı: Blokzincir yapısının sürdürülebilir olması ve bünyesine yeni blokların eklenmesi için düğümlere ihtiyaç duyulmaktadır. Herkese açık blokzincir yapılarında düğümlerin sisteme dahil edilmesi için teşvik protokolü bu katman üzerinde ele alınabilir.

Dağılım ve Transfer Katmanı: Bir blokzincirde hangi zincirin ana zincir olduğuna karar vermek ve kopmamak, bağımsız hareket etmemek ve aynı zamanda yeni blok üretiminde bu bilgiyi diğer bloklara iletmek gerekmektedir. Bu hususta düğümler arası iletişim oldukça önemlidir.

Doğrulama Katmanı: Blokzincirde üretilen yeni blokların önceki bloklar ile ne şekilde bağlanması, ilişkilendirilmesi gerektiğinin yanı sıra üretilen bu bloğun içerisindeki verini formatının uygunluğunu belirleyen protokoldür [26,33].

Uygulama Katmanı: Daha önce bahsedilen dört katman üzerine inşa edilmiş belirli bir para transferi ya da talep edilen bir fonksiyonun gerçekleştirildiği katmandır. Ek olarak içerik paylaşımı, görüntüleme gibi fonksiyonellikler servis çağrımları ile sağlanmaktadır [34,35].

2.2.3. Blokzinciri Önemli Yapan Özellikler

Blokzincir verileri belli ebatlarda bloklar halinde saklamaktadır. Bu bloklar birbirine bağlanarak büyümekte ve yeni oluşan blok kendisinden bir önceki bloğun SHA-256 özet değerini barındırmaktadır. Bir verinin değişikliğe uğraması içerisinde bulunan bloğun yeni bir özet değer üretmesine sebep olmaktadır. Bloktaki bu değişimin fark edilmemesi, geçerli olması ve tüm düğümler tarafından kabul görmesi için kendisinden sonra oluşan tüm blokların özet değerlerinin tekrardan hesaplanması gerekmektedir. Emeğin ispatı mutabakat yaklaşımın da ana düğümdeki bu blokların hepsinin değişimi yüksek maliyet, emek ve zaman gerektirmektedir. Değiştirilme zorluğu sebebiyle blokzincir yapısı içerisindeki bloklarda kayıt edilen veriler ölümsüz kabul edilmektedir. Bitcoin'de ECDSA algoritması kullanılarak sayısal imza üzerinden işlemler gerçekleştirilmektedir [36]. Günümüz teknolojisinde gizli anahtarlar üzerinden gerçekleştirilen işlemlerin taklit edilmesi oldukça zordur. Bu yaklaşım ile blokzincirdeki işlemin kimler tarafından gerçekleştirildiği, sahipliği net bir şekilde tespit edilebilmektedir. Bitcoin gibi, yapıları açık olarak tasarlanan blokzincir yaklaşımları sayesinde veriler herkesçe erişilebilir konumda olmaktadır.

2.4.4. Kayıt Edilebilen Data Türleri

Çoğunlukla blokzincir yapısı içerisindeki bloklarda işlem bilgisi ve akıllı sözleşmeler kayıt altına alınmaktadır. Fakat yeni yaklaşımlar ile Bitcoin işlemlerinin yapısında bulunan yazılabilir alanlara işlem bilgileri yanında sertifika, belge özetleri, dosya, resim ve zararlı yazılımlar da eklenebilmektedir [37]. 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 [9,38]. Diploma doğrulamada bu yaklaşım uygulanmaktadır.

2.3. Blockcerts

Blockcerts bünyesinde Resim.1'de gözüktüğü gibi diploma oluşturma, paylaşma ve doğrulama fonksiyonlarını barındırır.

Oluşturma: 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 Cert-tools ile JSON-LD formatında imzalanmamış dijital diploma oluşturulur. Sonrasında Cert-issuer ile üretilen diploma imzalanarak Bitcoin işlemlerinin yapısında bulunan OP_RETURN alanına diploma özeti eklemesi gerçekleştirilir. Bu işlem ile blokzincir yapısı içerisindeki bloklarda diploma özeti kayıt altına alınmış olur. Toplu diploma imzalamada Merkle Tree kullanılmaktadır [27].

Paylaşım: Üretilen imzalanmış diplomanın paylaşımı mail gibi farklı kanallar üzerinden paylaşılabilir veya link üzerinden diplomayı alan kişi bu diplomaya erişip geliştirilen android veya ios mobil uygulamalar ile diplomalarını bir yerde toplayabilir. Oluşturulan JSON-LD formatındaki diplomalar Cert-viewer ile html element üzerinden okunabilir bir şekilde gösterilebilmektedir.

Doğrulama: Cert-Verifier ile diplomanın özeti ve signature alanındaki Bitcoin işleminin yapısındaki OP_RETURN belirtecindeki değeri ile karşılaştırma yapılmaktadır. Karşılaştırma doğru ise veren ve alan kimlik birlikleri karşılaştırılır. Kimlik bilgileri doğrulaması akabinde diplomanın geçerlilik süresini, iptal durumunu kontrolleri ile doğrulama adımını tamamlar [9].

3. Türkiye'de Blokzincir Tabanlı Evrak Yönetimi Çözümü

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.

3.1. Türkiye'ye Standartlarına Uyumluluğu

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

Tablo 2. Diploma Alanlarının Kullanım Oranı.

Diploma Alanı	*Kullanım Oranı*	*Diploma Alanı*	*Kullanım Oranı*	*Diploma Alanı*	*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. TABLO II 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. Türkiye'deki üniversitelerin şeffaflığının artırılması, mezunların ulusal düzeyde iş bulma imkânının sağlanması ve tüm Avrupa'da kabul gören ortak diploma oluşturma amacıyla diploma eki verilmektedir [12,13,14]. 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: Programın türü, detaylı bilgi, alınan dersler/notlar/krediler, notlandırma, yetkinliğin sınıfı.
Yetkinliğin kullanım alanları: Üst dereceye başlama imkânı, meslek icra etme hakkı.
Ek bilgiler: Ek bilgi ve elde edilebilecek başka kaynaklar.

Analiz neticesinde Türkiye'de diploma üretiminde ihtiyaç duyulan nitelikler ile merkezsiz bir yapıda doğrulama imkânı sunan Blockcerts'in sertifika içerikleri karşılaştırılmıştır. Bu karşılaştırma sonucunda bazı ihtiyaçların mevcut JSON-LD tanımları içerisinde bulunmadığı tespit edilmiştir. Blockcerts'in Türkiye'de uyumlu çalışabilmesi için JSON-LD üzerinde ek ihtiyaç alanlarının tanımlanabiliyor olması gerekmektedir. Yapılan testler ve Cert-tools üzerinde yapılan ek geliştirmeler ile ihtiyaç duyulan niteliklerin tanımlandığı ve bu şekilde Bitcoin'nin blokzincir yapısı üzerinden doğrulama yapılabildiği gözlenmiştir. Türkiye standartlarına uygun Blockcerts'e ek nitelikler tanımlanarak diploma üretilebildiği görülmüştür. Böylelikle blokzincir teknolojisinin getirmiş olduğu kalıcılık ve güven ile birlikte Türkiye standartlarına uyumlu bir doğrulama metodunun gerçekleştirilmesi sağlanmıştır.

4. Sonuç

Diploma doğrulama sürecinin farklı yaklaşımları ele alınmış ve güvenilirliği yüksek olan blokzincir tabanlı çözümler üzerinden en sağlıklı bir şekilde doğrulamanın yapılabileceği ortaya konmuştur. Ülkemizde uygulanan diploma doğrulama süreçleri incelenmiş, mevcut yöntemlerin yerine daha kalıcı, uygulanabilir, hızlı ve daha güvenilir bir yapı üzerinden uyarlanmasının mümkün olabildiği gösterilmiştir. Blockcerts ile uluslararası bir düzeyde diploma doğrulama sürecine Türkiye'nin de dâhil olabileceği gösterilmiştir. Türkiye'de kullanımda olan diplomaların standartlarını incelememiz sonucunda merkezsiz daha güvenilir bir doğrulama adımlarını bünyesinde barındıran şeffaflık sağlayan açık kaynak kodlu yapısı gereği Blockcerts çözümünün Türkiye'nin diploma doğrulama süreçleri için kullanımına uygun olduğu sonucuna varılmıştır. Uyumluluk için gerekli ek alanların JSON-LD üzerinde gerçekleştirebilmemiz ile bu sürecin yapılabilirliği ortaya konulmuştur.

References

[1] D Diplomamakes. Welcome to Diploma Makers. (2018). https://diplomamakers.com Accessed 01 May 2018.

[2] Yeniakit. MEB'de sahte diploma skandalı! Tam 153 öğretmen. (2017). https://www.yeniakit.com.tr/haber/mebde-sahte-diploma-skandali-tam-153-ogretmen-278943.html Accessed 01 May 2018.

[3] T24. TÜBİTAK'ta ikinci sahte diploma skandalı!. (2015). http://t24.com.tr/haber/tubitakta-sahte-diploma-skandali,284377 Accessed 01 May 2018.

[4] E-Devlet. Yükseköğretim Mezun Belgesi Sorgulama. (2015). https://www.turkiye.gov.tr/yuksekogretim-mezun-belgesi-sorgulama Accessed 01 May 2018.

[5] Haber7. E- devlet'e erişimde sorun! BTK'dan açıklama geldi. (2017). http://www.haber7.com/teknoloji/haber/2401171-e-devlete-erisimde-sorun-btkdan-aciklama-geldi Accessed 01 May 2018.

[6] MIT. MIT Degree Verification. (2018). https://credentials.mit.edu/ Accessed 20 April 2018.

[7] Open Source University. The World's Academic & Career Development Ledger. (2018). https://os.university/ Accessed 05 April 2018.

[8] The University of Melbourne. Melbourne University to pilot a distributed database for micro-credentials. (2017). http://newsroom.melbourne.edu/news/melbourne-university-pilot-distributed-database-micro-credentials-0 Accessed 05 April 2018.

[9] Bockcerts. Blockcerts Universal Verifier. (2017). https://www.blockcerts.org/ Accessed 05 April 2018.

[10] YÖK. Yükseköğretim Mevzuatı. (2015). http://www.yok.gov.tr/web/guest/mevzuat Accessed 22 April 2018.
[11] Başbakanlık. Yükseköğretim Kanunu. (2018). http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.2547&MevzuatIliski=0&sourceXmlSearch= Accessed 22 April 2018.
[12] Guy Aelterman, Bruno Curvale, Armağan Erdoğan, Emmi Helle, Susanna Kärki, Charlotte Miles, Françoise Profit. (2009). Study on the Diploma Supplement as seen by its users. http://www.enqa.eu/indirme/papers-and-reports/associated-reports/Diploma%20Supplement%20Study_Edit%20MS.pdf Accessed 22 April 2018.
[13] Enic-Naric. The Diploma Supplement. (2018). http://www.enic-naric.net/fileusers/THE_DIPLOMA_SUPPLEMENT.pdf Accessed 05 May 2018.
[14] Newcastle University. Diploma Supplement. (2018). http://ncl.ac.uk/students/progress/assets/documents/HEAR.pdf Accessed 05 May 2018.
[15] İstanbul Üniversitesi. Diploma Eki. (2018). http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=diploma_eki.pdf Accessed 05 May 2018.
[16] IMS Global Learning Consortium. Open Badges v2.0. (2018). https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/index.html Accessed 05 May 2018.
[17] Haberturk. Bin liraya diploma!. (2011). http://www.haberturk.com/yasam/haber/586991-bin-liraya-diploma Accessed 05 May 2018.
[18] Sakarya Üniversitesi. Diploma Doğrulama Sistemi. (2018). http://www.ogrisl.sakarya.edu.tr/tr/icerik/9804/34476/diploma-sorgulama Accessed 05 May 2018.
[19] University Of Oxford. Verifying qualifications. (2018). https://www.ox.ac.uk/students/graduation/verification?wssl=1 Accessed 05 May 2018.
[20] University of Cambridge. Verification of Cambridge degrees. (2018). https://www.cambridgestudents.cam.ac.uk/your-course/graduation-and-what-next/verification-cambridge-degrees Accessed 05 May 2018.
[21] Qualificationcheck. Fast, secure education verifications. (2018). https://www.qualificationcheck.com Accessed 05 May 2018.
[22] edX. Earn Your Edx Verıfied Certıfıcate And Share It Wıth The World. (2018). https://www.edx.org/verified-certificate Accessed 05 May 2018.
[23] Sony Global Education. Creating a Trusted Experience with Blockchain. (2018). https://blockchain.sonyged.com/ Accessed 05 May 2018.
[24] CoinFirm. AMLT, The Token Of Complıance. (2018). https://www.trudatum.com/pdf/white-paper.pdf Accessed 05 May 2018.
[25] Gradbase Limited. Let's End Cv Fraud. For Good. (2018). https://gradba.se/en Accessed 05 May 2018.
[26] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. self-published pape. https://bitcoin.org/bitcoin.pdf
[27] R.C. Merkle. (1980). Protocols for public key cryptosystems. http://www.merkle.com/papers/Protocols.pdf
[28] David Xiao. The Four Layers of the Blockchain. (2016). https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f Accessed 05 May 2018.
[29] Github Etherium. Proof of Stake FAQ. (2016). https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ Accessed 05 May 2018.

[30] Slimcoin. A Peer-to-Peer Crypto-Currency with Proof-of-Burn. (2018). https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf Accessed 05 May 2018.
[31] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak. Proofs of Space. (2013). https://eprint.iacr.org/2013/796.pdf Accessed 05 May 2018.
[32] A. Back. (2002). Hashcash - a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf Accessed 01 May 2018.
[33] Decker, C and Wattenhofer R. (2013). Information Propagation in the Bitcoin Network.
[34] Github Bitcoin. Bitcoin. (2018). https://github.com/bitcoin/bitcoin Accessed 05 May 2018.
[35] Github Ethereum. Ethereum. (2018). https://github.com/ethereum/ Accessed 05 May 2018.
[36] Bitcoin. (2017). https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm Accessed 01 May 2018.
[37] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Mu¨llmann, Oliver Hohlfeld, and Klaus Wehrle. (2018). A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf Accessed 02 May 2018.
[38] Bernstein. Intellectual property for the digital age. (2018). https://www.bernstein.io Accessed 06 May 2018.
[39] İstanbul Şehir Üniversitesi. İstanbul Şehir Üniversitesi Önlisans Ve Lisans Eğitim-Öğretim Ve Sinav Yönetmeliği. (2018). https://www.sehir.edu.tr/tr/Documents/Yonetmelikler/IstanbulSehirUniversitesiOnlisansLisansEgitimOgretimSinavYonetmeligi20170219.pdf Accessed 06 May 2018.
[40] Sakarya Üniversitesi. Diploma, Mezuniyet Belgesi İle Diğer Belgelerin Düzenlenmesinde Uyulacak Esaslara İlişkin Yönerge. (2018). http://www.ogrisl.sakarya.edu.tr/tr/icerik/8852/31931/diploma-yonergesi Accessed 06 May 2018.
[41] Uludağ Üniversitesi. Önlisans Ve Lisans Öğretim Yönetmeliği. (2017). http://www.uludag.edu.tr/dosyalar/ysehirmyo/duyuru_dosyalar/y%C3%B6netmelik%2012.01.2017.pdf Accessed 06 May 2018.
[42] Blockchainhub. Blockchains & Distributed Ledger Technologies. (2018). https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/ Accessed 11 May 2018.