Blok Zinciri İle Gerçek Zamanlı Doğrulanabilir Eğitim Belgeleri[1]

Doruk AYBERKİN[2]

Bayburt Üniversitesi, Teknik Bilimler Meslek Yüksekokulu

Mansur BEŞTAŞ[3]

Siirt Üniversitesi

Üstün ÖZEN[4]

Atatürk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi

ÖZET

Blok zinciri, sayısallaştırılmış bilgilerin bir ağ üzerinde farklı düğümlere kayıt edilmesi, kayıt edilen bilgilerin diğer düğümlerle de paylaşılarak doğrulanabilir ve şeffaf olmasını sağlayan yapıdır. Ağ üzerinde dağıtık yapıda bulunan düğümlerin her biri programlar vasıtasıyla ağ üzerindeki işlemleri takip eder. Akıllı kontratlar sayesinde işlemlerin doğruluğu kontrol edilerek her bir düğümün dağıtılmış defteri güncellenir ve özdeş bir kopya olarak tüm düğümlere kayıt edilir. Düğümler yapı içerisinde bulunan şifreleme ve ağaç yapısı sayesinde, yeni düzenlemelerin veya girişlerin nasıl başlatıldığını, onaylandığını, kaydedildiğini ve dağıtıldığını izleyebilir, ancak tek başlarına müdahale de bulunamazlar. Sistem merkezcilikten uzak üst düzeyde güvenilir bir yapıdadır ki bu sayede güvene dayalı sektörlerde ilgi uyandırmıştır. Sıklıkla sahtecilikle karşılaşılan eğitim belgelerinin güvenirliğini sağlamak ve gerçek zamanlı doğrulama işlemlerini gerçekleştirebilmek için de Blok zinciri ile çalışmalara başlanmıştır. Bu çalışmada amaç; Blok zincirinin özellikleri, gelişimi ve işleyiş yöntemini kısaca tanıtarak, eğitim belgelerinin anlık olarak doğrulanmasının önemi ve bu doğrulama için blok zincirinin nasıl kullanılabileceği sorularına cevap vererek blok zinciri tabanlı bir uygulama kurgusu oluşturmaktır.

Anahtar Kelimeler: *Blok Zinciri, Akıllı Kontrat, Eğitim, Eğitim Sertifikaları*
Jel Sınıflandırması: I29, C89

[1] ***Bu çalışma "Uluslararası Uygulamamalı İşletme Yönetim ve Ekonomi Araştırmaları 2018 Sempozyumu"nda sunulmuştur.***

[2]Öğr. Gör., Bilgisayar Programcılığı, Bayburt Üniversitesi, E-Posta: doruk@bayburt.edu.tr, ORCID: 0000-0003-3409-8926

[3] Siirt Üniversitesi Bilgi İşlem Şube Müd., E-Posta: mansur@siirt.edu.tr, ORCID: 0000-0002-8192-2044

[4] Prof. Dr., Atatürk Üniversitesi, İİBF, Yönetim Bilişim Sistemleri Bölümü, E-Posta: uozen@atauni.edu.tr, ORCID: 0000-0002-7595-4306

1. GİRİŞ

Türkiye'de, TÜİK Ulusal Eğitim İstatistikleri Veri tabanına göre 2016 yılında yaklaşık 4,7 milyon öğrencinin lise ve dengi okullarla, üniversitelerden mezun olarak bir eğitim belgesine sahip olduğu ve bu sayının her yıl artarak devam edeceğini öngörülmektedir. Buna ek olarak, iş hayatında resmi bir eğitim kurumundan alınmamış eğitim belgeleri ve diğer sertifikalar da eğitim belgesi statüsünde işlem görmektedir. Eğitim belgesi sahiplerinin çoğunun her yıl iş başvurusunda bulunduğu düşünüldüğünde işverenlerin bu bilgileri doğrulaması ihtiyacı eskiden olduğu gibi gelecekte de büyük bir iş yükü olarak karşılarına çıkacaktır.

Eğitim belgelerine sahip olma süreci ülkelere ve eğitim kurumlarına göre değişen bir süreçtir. Alınan belgeler, belgenin sağlayıcısı eğitim merkezi tarafından hızlı ve güvenilir bir biçimde, çevrimiçi olarak kontrol edilebilmektedir. Ancak daha yakın zamanda ortaya çıkan, 20 yıla yakın süredir diplomasız öğretmenlik yapan bir kadın haberi eğitim belgelerinin kontrolünün önemli olduğunu bir kez daha göz önüne sermiştir. (CnnTurk, 2017) Ayrıca bazı internet siteleri kullanıcıların isteklerine göre ücret karşılığı sahte diploma üretebilmektedir. (Sahte diploma, 2017)

Şu an ülkemizde hali hazırda kamu kurumları çevrimiçi sistem e-devlet kapısı üzerinden belge sorgulaması yapabilmektedir. (E-Devlet, 2017)Ancak sistem tek bir merkezden yönetildiğinden sisteme erişimi olan kullanıcıların kötü niyetli işlemler yapmayacağının garantisi yoktur. Ayrıca resmi olmayan eğitim merkezlerinden alınan diplomalar, E-Devlet üzerinden sorgulanabilir değildir.

Verinin olduğu her ortamda, verinin doğruluğu ve bütünlüğü problem olarak devam etmiştir ve edecektir. Şifreleme teknikleri ile oluşturulan güvenlik mekanizmalarında her zaman üçüncü bir tarafın verinin güvenirliliği için referans noktası olması durumu ile karşı karşıya kalınmıştır. Bu durum kendi içinde zayıflıklar ortaya çıkarmaktadır. Bu şifrelemenin doğasında bulunan bir durumdur. Bu duruma çözüm olarak - Üçüncü bir tarafın referans olması gerekliliğini ortadan kaldıran blok zinciri teknolojisi gittikçe daha fazla alanda kullanılmaya başlamıştır.

Blok zinciri teknolojisinin belge doğrulama sistemi ile bütünleştirilmesi sayesinde kontrol mekanizmasındaki merkeziyetçilik ortadan kaldırılarak kullanıcı inisiyatifi ortadan kaldırılabilir. Ayrıca mevcut sistemlerde belgeleri doğrulama görevi uzun zaman alan bir işlemdir. İşlem belge sağlayıcısının verdiği cevaba bağlı olarak birkaç haftadan aylara kadar sürebilir. Blok zinciri sayesinde belge doğrulaması yapmak isteyen işverenler ya da kurumlar maliyet ve zaman harcamak durumunda kalmadan işlemlerini gerçekleştirebileceklerdir.

2. LİTERATÜR TARAMASI

Tarih boyunca değerli evrakların saklanması ve doğrulanması için sürekli çaba içerisinde olunmuştur. Bilginin içeriğinin doğruluğu ve değiştirilmediği önemli bir noktadır. Verinin şifrelenmesi, 20. Yüzyıla kadar basit alet ve edevat kullanılarak yapılmaktaydı. Antik Yunan ve Spartalılarda Skytale ismi verilen tahta bir araç ile üzerine sarılan deri şeride mesajın yazılması ile gerçekleştirilmekte idi. Şerit Skytale üzerinden alındığında barındırdığı mesajın harfleri karmaşık hale gelmekte ancak mesaj aynı ölçülerde Skytale ile anlamlı hale gelebilmektedir (Linkedin, 12). Karmaşık şifreleme yöntemlerinin gelişimi ilk olarak mekanik daha sonra elektromekanik imkânların artması ile ivme kazanmıştır.

Blok zinciri kavramı ilk olarak 2008 yılında Satoshi Nakamoto tarafından yazılan bir teknik makale ile ortaya çıktı. Makale bir aracıya bağlı olmadan eşler arasında güven esaslı bir değişim yapılabileceğini ve bu işlemlerin dağıtık defterlerde tutulabileceğini öngörmekteydi. (Nakamoto, 2017)

Blok zinciri gelişim açısından 3 aşamada incelenebilir. Blok zincirinin 1.0 versiyonu, sadece para transferi, havale ve dijital ödeme sistemleri gibi kripto para birimleri ile ilgili

uygulamalarda kullanılmıştır. Blok zincirinin 2.0 versiyonu, akıllı sözleşmelerin gelişmesi ile birlikte basit para işlemlerinden daha kapsamlı bir biçimde, hisse senetleri, tahviller, vadeli işlemler, krediler, ipotek gibi piyasalarda ve finansal işlemlerde kullanılmıştır. Blok zincirinin 3.0 versiyonu ise para, maliye ve piyasaların ötesinde, özellikle hükümet, sağlık, bilim, edebiyat, kültür ve sanat alanlarındaki blok zincir uygulamalarında kullanılmaktadır. (Swan, 2015)

Blok zinciri teknolojisi toplumsal, ekonomik ve kamusal alanları etkileme potansiyeline sahiptir. (Flament, 2015) Blok zinciri eğitim alanında, eğitim belgeleri ve sertifika gibi kayıtların saklamak için kullanılabilir. Eğitim verisi, belgeyi sağlayan kurum tarafından blok zincirine eklenir. Bu zincir verilere anahtara sahip kullanıcıların erişebildiği, işverenlerle paylaştığı çevrimiçi bir sistemdir. Blok zinciri kurumdaki değişikliklere karşı korunan veya özel kayıtlarının kaybolmasına karşı sürekli bir kamusal kayıt sağlar. (Sharples & Domingue, 2016)

Bu amaçla çeşitli çalışmalar yapılmaya başlanmıştır. Ortaya çıkan ilk örneklerden birisi checkdiploma.org 'dur (checkdiploma, 2017). Etherium ağı üzerinde akıllı sözleşme olarak diploma bilgisinin saklanması yöntemi ile bu konuya çözüm üretmeye çalışmıştır.

Lefkoşa Üniversitesi, Bitcoin blok zinciri aracılığıyla özgünlüğü doğrulanabilen akademik sertifikalar üreten ilk yükseköğrenim kurumudur. ((UNIC), 2017)Lefkoşa üniversitesi ayrıca sistemin kodlarını açık kaynak olarak da çevrimiçi yayınlayarak kamunun kullanımına açmıştır. MIT üniversitesi pilot program olarak 2017 yılı yazında blok zincir teknolojisi üzerinde çalışan sertifika doğrulama hizmetini devreye almıştır (blockcerts, 2017). Mezunlarına diplomaları ile birlikte mobil ortamda diplomalarını doğrulayabilecekleri mobil uygulama ve blok zincir bilgisini vermiştir (MIT News, 2017). MIT geliştirdiği teknolojiyi MIT lisansı ile 2017 yılında kamuya açmış bulunmaktadır (Github Blockcerts, 2017).

Günümüzde blok zinciri teknolojisini kullanan sistemler giderek artmaktadır.

3. BLOK ZİNCİRİNİN GELİŞİMİ, ÖZELLİKLERİ, İŞLEYİŞ ŞEKLİ

Anonim bir kişiliğe sahip olan Satoshi Nakamoto, 2008'de "Bitcoin: Eşler arasın elektronik ödeme sistemi" adında bir rapor yayınladı. (Nakamoto, 2017) Raporda ilk defa blok zinciri kavramı detaylarıyla anlatılmıştır.

Blok zinciri, çok sayıda bağımsız kullanıcı tarafından korunan genel bir çıktı olarak da ele alınabilen dağıtılmış bir veri tabanı sistemidir. Bir işlem bir blokta yazıldığında, işlem verilerinin sistemdeki tüm düğümler tarafından anlaşılması gerekir ve veriler herhangi bir düğüm tarafından değiştirilemez. Tüm düğümlerin antlaşması akıllı kontrat sistemi ile gerçekleştirilir. Zincirdeki bir bloğun verileri yasa dışı olarak değiştirilirse, bu zincirin ardından zincirin tamamı etkilenir ve diğer düğümler zincirdeki verilerin geçerliliğini kabul etmez. Sistemdeki katılımcılar veya düğümlerin birbirlerini tanımaları ya da birbirlerine güvenmeleri gerekmez. Dahası, tüm sistem kuralları genel ve şeffaftır. Aynı zamanda bu kurallar tüm düğümler tarafından kabul edilir. Her düğüm, tüm blok tabanlı zincirde saklanan tüm verilerin özdeş bir kaydını tutar. Diğer bir deyişle, her düğüm, veri tabanının tek bir düğüm tarafından ayrı ayrı değiştirilemeyeceğini garanti eden bir veri tabanının kopyasını tutar. Kriptografi ile bağlantılı zincir biçimindeki blokların mimarisi, dağıtılmış güvenliği sağlar. Sistemde tüm işlemler zaman damgalı bloklar halinde gruplandırılmıştır ve her grup bir önceki zaman damgasını da içerir.

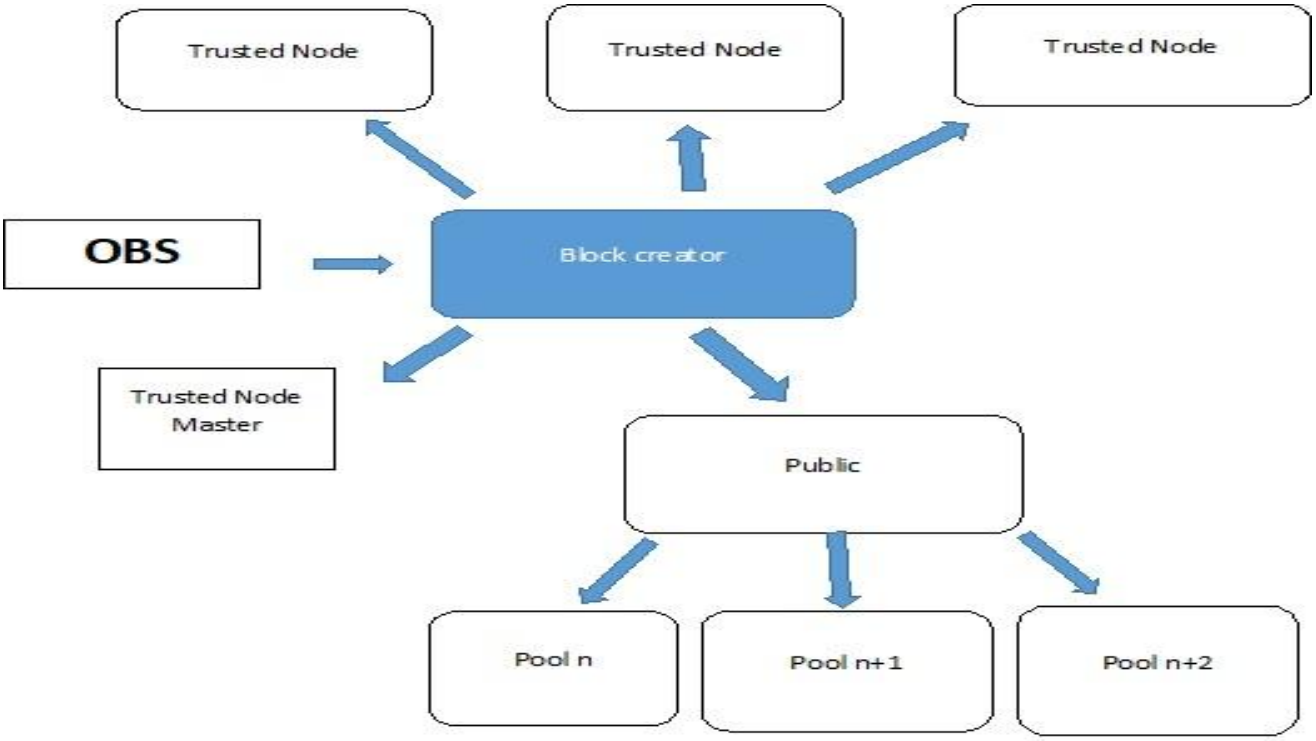
Blok zinciri içerisinde birden çok kavramı barındıran karmaşık bir yapıdır. Bu yapılardan aşağıda kısaca bahsedilmiştir.

Dağıtık Kayıt Defterleri tüm işlemlerin tam listesini içeren veri tabanlarıdır. Deftere sahip blok zincirinin tüm kullanıcıları ağdaki tüm işlemlerin sürekli güncellenmiş bir sürümüne

sahiptir. Defter her kullanıcı tarafından erişilebilir, evrensel, müdahale edilemez ve merkezi otoriteden bağımsızdır. (Swan, 2015)
Kayıt defterlerinde her bir kullanıcının sahip olduğu kayıtların özdeş olabilmesi için aralarında bir kanıtlama mekanizması gerekir. Bu mekanizmaların en çok kullanılan iki tanesi iş kanıtı(Proof of Work (PoW) ve Proof of Stake (PoS)'dir.Proof of Work mekanizmasında yeni blokların kabul edilmesi için kriptografik ispat belgeleri gereklidir. İşlemleri doğrulamak ve işlem kanıtını hesaplamak için yüksek işlem güçlerine ihtiyaç duyulur ve bloğu bulan sistemdeki kripto para ile ödüllendirilir. İş ispatı için matematiksel algoritmalardan yararlanılır. Proof of Stake' ise ikili bir protokole dayanıyor. Bu protokolde işlem gücünden öte sistemde en eski olan ve elinde kripto para bulunduran bir destekçi yardımıyla işlemler tamamlanır. (Usta & Doğantekin, 2017)
Her iki protokolün de finali, hangi bloğun zincirin yanında eklenmesi gerektiği üzerinde fikir birliğine varmak için kullanılır. (Pilkington, 2015)
Dağıtık kayıt defterlerindeki veriler kriptografik hash ile tutulurlar. Bu yaklaşım temel olarak matematiksel işlemler kullanarak büyük bir veriden kıyasla daha küçük bir özet bilgi üretilmesidir. Tek yönlü olarak çalışır yani, özet bilgiden kaynak veriye geri dönülemez. Şifrelenmiş olan bu veriler Merkle ağaçlarında taşınır. Bu ağaçlar sayesinde veriler güvenli ve hızlı bir şekilde doğrulanabilmektedir. (Usta & Doğantekin, 2017)
Her blok işlemin yapıldığı zamanı belirlemek için bir zaman damgası barındırır. Zaman damgası verilerin işaretlenen tarihte olduğunun kanıtıdır ve bir belgenin varlığını güvence altına alabilir. (Swan, 2015)
Akıllı sözleşmeler bloklar içerisinde saklanan kod parçalarıdır. Blok zincirindeki işlemin insan katılımı olmaksızın nasıl çalışması gerektiğine ilişkin talimatları içeren basit işlemlerdir. Sözleşmede tüm tarafların kabul ettiği koşullar belirtilir ve şartlar sağlandığında ortaya çıkacak işlemler kayıt altına alınır. (Swan, 2015) (Usta & Doğantekin, 2017)

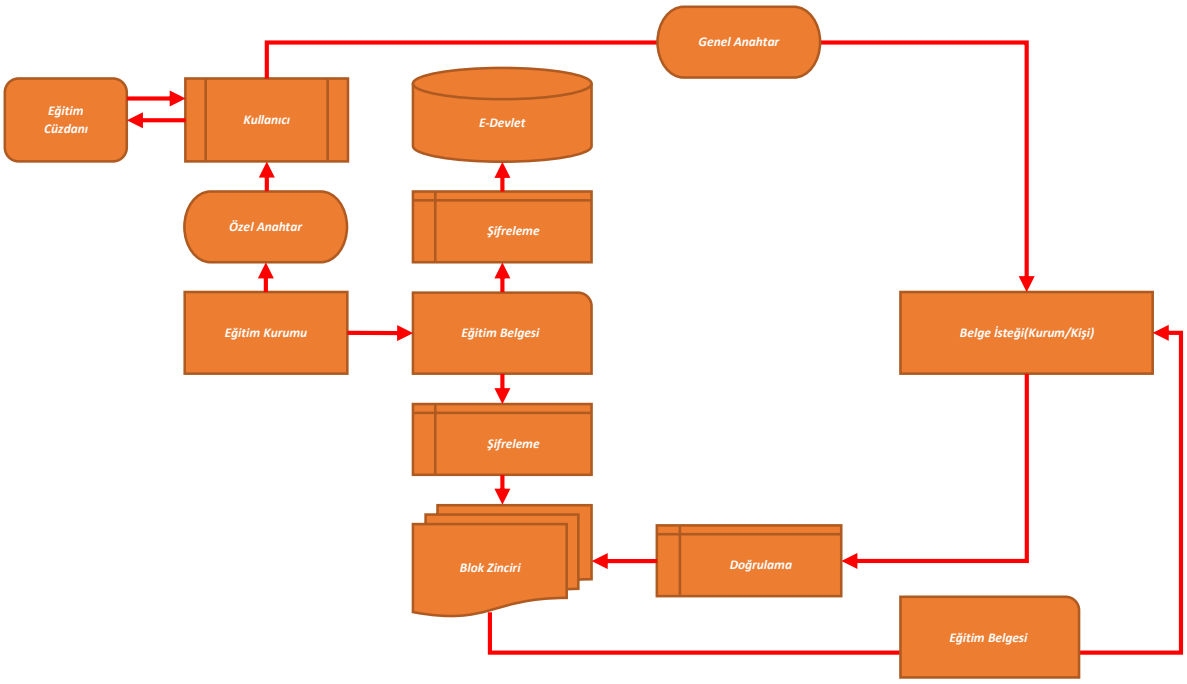
4. YÖNTEM

Eğitim kurumlarında öğretim ve eğitim alan bireyler, hedeflenen bilişsel ya da yeteneksel kazanımları tamamladıklarında bu durumlarını ihtiyaç duyulan mercilerde kanıtlamak amacıyla belge alırlar. Bu belgelendirmenin ilk örneklerini batı Asya coğrafyasında medreselerde icazet müessesi ile görebiliriz. Eğitim belgesinin doğrulanabilir ve değiştirilemez olduğuna yönelik metot çalışmamız şu şekildedir:
Bireyin eğitim aldığı öğretim kurumu diploma bilgisini blok zincir oluşturan referans kuruma iletir. Bu kurum bilgiyi gerekli şekilde özet bilgisini alarak zincir Hash değeri olarak belirler. Ardından bir önceki blok için oluşturulmuş olan bloğun Hash değerini ekleyerek zincir yapısını oluşturur. Oluşturulan yeni blok bilgisi yayın olarak verilir. Yayın olarak verilmesinin nedeni blokların oluşturduğu zincir yapısını saklamak isteyen düğüm noktalarına bilgi vermektir. Önerilen metotta her yükseköğretim kurumu oluşturulan zincirin bir kopyasının kendi bünyesinde saklaması önerilmektedir. Bununla beraber eğer var ise yükseköğretim kurumlarının koordinasyon kurumu ya da milli eğitiminden sorumlu tüzel kurum zincirin bir kopyasının saklar. Yükseköğretim kurumları trustedNode olarak adlandırılmıştır. Yükseköğretimden sorumlu koordinasyon kurumu masterNode olarak ifade edilmiştir. Blok zinciri yayın olarak verildiğinden dolayı isteyen bireysel ya da kurumsal kullanıcılar zincirin bir kopyasını saklayabilir. Ülke içerisinde yapı bu şekilde iken isteyen ya da dünya çapında çapta her ülkenin Blok zincir bilgisini tutan birkaç düğüm noktası (Node) oluşturulabilir.
Bu şekilde oluşturulacak bir yapıda diploma bilgisi değiştirilemez ve doğrulanabilir bir yapıda gerek coğrafik gerekse teknolojik altyapısal olarak dağıtılmış olacaktır. Verinin yani diploma içeriğinin doğrulanması için üçüncü bir tarafa ihtiyaç olma gereksinimi ortadan kalkmıştır.



Şekil 1. Önerilen sistem modeli

Önerdiğimiz sistem, eğitim bilgilerini ihtiyaç duyulan kurumların ağıyla paylaşarak kaydeder. Blok zinciri kullanılarak platformdaki eğitim belgeleri doğrulanır. Bu sayede eğitim kurumları ve kişiler oluşturulan her bir eğitim belgesinin doğruluğunu hızlı ve kolayca belirlemek için kullanabilir. Buna ek olarak, sistemi kullanan kurum ve kişiler, farklı taraflarca sunulan bilgilere tek bir noktadan ulaşarak tarafların dijital belgeleri birbirleriyle güvenilir şekilde paylaşmalarını sağlayabilirler.



Şekil 2. Araştırmanın uygulama modeli

5. SONUÇ

Dünya üzerinde teknolojik gelişmelerin mekânsal sınırları kaldırması ile beraber zamansal sınırları azaltması sonucu verinin değiştirilemez, doğrulanabilir ve sürekli erişilebilir olması ihtiyacı ortaya çıkmıştır. Teknoloji bir değer olarak yükselen blok zincir yapısı beraberinde geniş teknik uygulama alanları sağlamaktadır. Bu çalışmada önerilen metot temellerini blok zincir yapısından almaktadır.

Blok zinciri teknolojisi toplumsal, ekonomik ve kamusal alanları etkileme potansiyeline sahiptir (Flament, 2015). Blok zinciri eğitim alanında, eğitim belgeleri ve sertifika gibi kayıtların saklamak için kullanılabilir. Eğitim verisi, belgeyi sağlayan kurum tarafından blok zincirine eklenir. Bu zincir verilere anahtara sahip kullanıcıların erişebildiği, işverenlerle paylaştığı çevrimiçi bir sistemdir. Blok zinciri kurumdaki değişikliklere karşı korunan veya özel kayıtlarının kaybolmasına karşı sürekli bir kamusal kayıt sağlar (Sharples & Domingue, 2016).

Bir veri olarak diplomaların dağıtık yapı içerisinde saklanması, diploma veren merciinin kapanması veya erişilebilirliğinin ortadan kalkması durumlarına karşı güçlü bir yapıya sahip olacaktır. Verinin blok zincir yapısı ile saklanmasından dolayı değiştirilmesi imkânsıza yakın bir ihtimaldir ve bu şekilde veriler güvence altına alınmaktadır.

Blok zinciri üzerinde diplomaların saklanması, evrak sahteciliği, erişilebilirlik, veri doğrulaması ve verinin yedekli bir biçimde saklanabilmesi avantajlarını da beraberinde getirmekte olup, uygulanabilir bir yöntemdir. Bir diğer taraftan dağıtık yapısı sayesinde veri merkezlerinin yükünü azaltması ve iletişim sorunsalını ortadan kaldırması, sayısal bir veri olması sayesinde baskı maliyetlerini ortadan kaldırması hususları göz önüne alındığında finansal olarak bir katkı sağlayacağı da görülmektedir. Çalışma bu yanıyla blok zinciri uygulamalarının maliyet katkısını görmek için yapılacak olan çalışmalara da fikir verecektir.

KAYNAKLAR

blockcerts. (2017, 12 13). blockcerts: http://www.blockcerts.org/ adresinden alındı

checkdiploma. (2017, 12 13). checkdiploma: https://checkdiploma.org adresinden alındı

CnnTurk. (2017, 12 10). (https://www.cnnturk.com/turkiye/sahte-diplomali-ogretmen-beraat etti) adresinden alındı

E-Devlet. (2017, 11 26). https://www.turkiye.gov.tr/yuksekogretim-mezun-belgesi sorgulama adresinden alındı

Flament, C. (2015). *Blockchain technology: A general purpose technology for the decentralization of governance?* ULB - Solvay Business School.

Github Blockcerts. (2017, 12 13). Github: https://github.com/blockchain-certificates adresinden alındı

Linkedin. (12, 12 2017). Linkedin: https://tr.linkedin.com/pulse/kriptografide-%C5%9Fifreleme-teknikleri-nihal-kindap adresinden alındı

MIT News. (2017, 12 13). Massachusetts Institute of Technology: http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017 adresinden alındı

Nakamoto, S. (2017, 11 29). bitcoin.org/: https://bitcoin.org/bitcoin.pdf adresinden alındı

Pilkington, M. (2015). *Blockchain Technology: Principles and Applications.* Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016.

Sahte diploma. (2017, 12 3). http://www.phonydiploma.com/ adresinden alındı

Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. *Adaptive and Adaptable Learning. EC-TEL 2016*, (s. 490-496). doi:https://doi.org/10.1007/978-3-319-45153-4_48

Swan, M. (2015). *Blockchain blueprint for a new economy.* O'Reilly Media, Inc.

UNIC, U. o. (2017, 12 20). *Block.co*. http://block.co/our-approach/: http://block.co/our-approach/ adresinden alındı

Usta, A., & Doğantekin, S. (2017). *Blockchain 101*. İstanbul: Kapital Medya Hizmetleri A.Ş.

Real-Tıme Verifiable Educational Certificates With Block Chain

Doruk AYBERKİN[1]

Bayburt University

Mansur BEŞTAŞ[2]

Siirt Üniversitesi

Üstün ÖZEN[3]

Atatürk University, Faculty of Economics and Administrative Sciences

ABSTRACT

The block chain is a structure that allows digitized information to be recorded on different nodes on a network, allowing the recorded information to be shared with other nodes to be verifiable and transparent. Each node in the distributed structure on the network monitors the operations on the network through the programs. Intelligent contracts control the accuracy of transactions, updating the distributed book of each node and registering it as an identical copy in all nodes. With the encryption and tree structure in the system, nodes can track how new edits or entries are initiated, acknowledged, saved and distributed, but they can not intervene on their own. Since the system is highly reliable at a distance from centrality, it has attracted interest in the trust-based sectors. Working with the block chain has also been started to ensure the reliability of educational certificates, which are often subject to fraud, and to perform real-time validation processes. The purpose of this study is to create a block-chain based application framework by briefly introducing the characteristics, development and operation methods of the block chain, expressing the importance of instant verification of the educational certificates and how block chain can be used for this verification.

Keywords: *Block Chain, Smart Contract, Education, Certificates*
Jel Classfication: I29, C89