International Journal of Engineering and Innovative Research

http://dergipark.gov.tr/ijeir

BLOK ZİNCİR TEMELLİ GÜVENLİ ELEKTRONİK OYLAMA MODELİ

Remzi GÜRFİDAN[1*], Zekeriya AKÇAY [2]

[1] Isparta Uygulamalı Bilimler Üniversitesi, Yalvaç Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Programcılığı Bölümü, Isparta, Türkiye.
[2] Gül Mesleki ve Teknik Anadolu Lisesi, Bilişim Teknolojileri Bölümü, Isparta, Türkiye.

https://doi.org/10.47933/ijeir.746235

*Sorumlu Yazar: remzigurfidan@isparta.edu.tr
(**Received:** 15.05.2020; **Revised**: 03.06.2020; **Accepted:** 15.06.2020)

ÖZET: Günümüzde bir konunun araştırılması, toplumun görüşünün alınması ya da tutumunun tespit edilebilmesi için araştırma anketleri, yüz yüze danışma, telefon görüşmeleri, web anketleri gibi çeşitli yöntemler kullanılmaktadır. Bu yöntemlerden en hızlı ve düşük maliyetli olan yöntem web anketleridir. Günümüzde küresel bazda yaşanan Covid-19 bulaş hastalığının kalabalık alanlarda yarattığı riskler göz önünde bulundurulduğunda web üzerinde çalışan sistemler hayati öneme sahiptir. Web anketi tercih edildiğinde sunucu tabanlı çalışan web uygulamaları kullanılmaktadır. Fakat sunucu tabanlı uygulamalar veri güvenliği ile ilgili bazı endişeler oluşmasına sebep olabilmektedirler. İstemci düğümlerinden sunucuya gönderilen oylama bilgileri, merkezi bir sunucu üzerindeki veri tabanına kaydedilmektedir. Verinin merkezi bir sunucu üzerinde depolanması yönteminin en büyük dezavantajı, oylama sonuçlarının siber saldırılar ya da kurcalanma risklerine savunmasız olmasıdır. Bu durum yapılan oylama sonuçlarının güvenliğini ciddi oranda olumsuz etkilemektedir. Blok zincir teknolojisi son yıllarda veri güvenliği alanında sıkça kullanılmaktadır. Blok zincir teknolojisinde sistemi merkezi bir sunucu yönetmemektedir. Eşler arası ağ oluşturulup hesap defterinin tamamının bütün düğümlerde yer alması prensibi esastır. Bu yapısı ile veri güvenliği açısından avantajlı bir teknolojidir. Ayrıca blok zincir teknolojisi, verilerin tek bir blok olarak şifrelenmesinden dolayı siber saldırılara ve dış müdahalelere karşı da güvenli durumdadır. Bu çalışmada farklı fikir ya da görüşlerin oylanması, oylama sonuçların gösterilmesi için blok zincir temelli güvenli bir elektronik oylama modeli önerilmiştir. Çalışmada C# dilinde blok zincir yapısı oluşturularak düğümlerden kullanılan oy verilerinin bir blok olarak şifrelenmesi ve bloğun zincire eklenmesi sağlanmıştır. Blok zincir tabanlı geliştirilen sistemin güvenli ve güvenilir olmasını, seçimde bulunan insanların güvenini artırmaya yardımcı olmasını bekliyoruz.

Anahtar Kelimeler: Blok Zincir, Veri Güvenliği, Elektronik Oylama Sistemi.

BLOCK CHAIN BASED SAFE ELECTRONIC VOTING MODEL

ABSTRACT: Today, various methods such as research questionnaires, face to face consultation, telephone interviews, web surveys are used to investigate a subject, to get the opinion of the society or to determine its attitude. The fastest and most cost effective method among these methods is web surveys. Given the risks posed by Covid-19 infectious disease on a global basis today in crowded areas, systems operating on the web are vital. When web survey is preferred, server based web applications are used. However, server-based applications may raise some concerns about data security. Voting information sent from the client nodes to the server is recorded in the database on a central server. The biggest disadvantage of the method of storing data on a central server is that the voting results are vulnerable to cyber attacks or tampering risks. This situation adversely affects the security of the voting results. Blockchain technology has been used frequently in the field of data security in recent years. In blockchain technology, the system does not manage a central server. The principle of establishing a peer-to-peer network and placing the entire ledger in all nodes is essential. With this structure, it is an advantageous technology in terms of data security. In addition, blockchain technology is also safe from cyber attacks and tampers due to the encryption of data as a single block. In this study, a secure electronic voting model based on block

chains has been proposed for voting different opinions or opinions and showing voting results. In the study, by creating a block chain structure in C # language, the data used from the nodes are encrypted as a block and the block is added to the chain. We expect the system developed based on block chains to be safe and reliable, helping to increase the trust of the people in the election.

Keywords: Blockchain, Data Security, Electronic Voting System.

1. GİRİŞ

Çalışma hayatında iş görenler yürüttükleri görev ile ilgili farklı problemler ile karşılaşmaktadırlar. Karşılaşılan problemler iş görenin yetki ve tecrübesine bağlı olarak aşılabilmekte ya da en optimize çözüme ulaşma amacıyla fikir danışma yöntemi ile aşılmaya çalışılmaktadır. İş görenler çözüm bekleyen problem senaryolarına farklı çözüm önerileri getirebilmektedirler. Bu tür durumlarda çözüm için uygulanacak yöntemin seçimi oyçokluğu ya da oybirliği ile belirlenebilir. Bu aşamada yaşanabilecek önemli problemlerden biri, oylama esnasında üyenin kendini baskı altında hissetmeden özgür irade ile gerçek düşüncesini ortaya koyabilmesidir. Bireyler düşündükleri fikrin diğer kişiler tarafından bilinmesini istemeyebilir.

Bu problem senaryosundan yola çıkarak bu problemin yaşanabileceği farklı durumlara da senaryolar genişletilebilir. Örnekleri çoğaltacak olursak, bir holdingin yatırım kararlarının belirlenmesi, bir şirketin çalışanlarına uyguladığı memnuniyet anketleri, bakanlıkların çalışan personeline uyguladığı kurum iklim anketleri, ülke çapında uygulanan yerel seçimler, genel seçimler, referandumlar örnek gösterilebilir. Özellikle referandum, genel ve veya yerel seçimler söz konusu olduğunda mali anlamda yaşanan giderlerin tasarrufu konusunda problemin yaygın etkisi ortaya çıkmaktadır. Problem senaryosunun yaygın etkisine arttıkça, senaryo paydaşlarının görüşlerin öğrenilmesi için harcanan mali tutar artmaktadır.

Kamuoyunun bir konu hakkında düşünce, kanaat ve eğilimlerini öğrenmenin en iyi yolu kamuoyu araştırmalarıdır. Kamuoyu araştırmaları dünyada 19. Yüzyılda ülkemizde ise 1960'lı yıllarda uygulanmaya başlanmıştır. Kamuoyu araştırmaları Türkiye'de 1980'li yıllardan sonra önemini arttırmıştır. İlk araştırmalar 1960'lı yıllarda yapılsa da kapsamlı araştırmalar 1975 yılında başlamış ama yaygınlaşması 1980 sonrasında olmuştur. Kamuoyu araştırmaları sayesinde seçmenlerin siyasî kanaat ve tutumları, gündem konularına yaklaşımı, siyasi lider ve adaylara duydukları ilgi, hangi medya ve medyaları kullandıkları belirlenebilmektedir. Seçmen tercihlerini öğrenmek için siyasiler kamuoyu araştırmalarını sıklıkla kullanmaktadırlar [1].

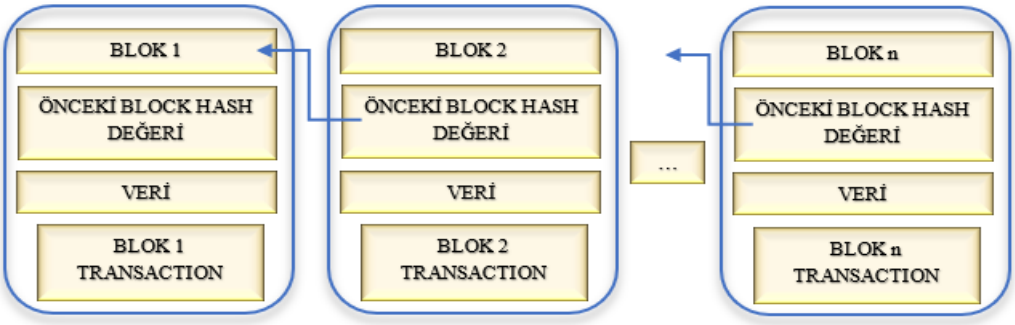
A.H. Eroğlu ve S. Bayraktar kamuoyu araştırmalarının seçmen davranışını yönlendirmek için de kullanılabildiği sonucuna ulaşmışlardır. Yapılan siyasi kamuoyu araştırmalarının seçmene iki farklı yoldan etki ettiğini belirtilmiştir. İlk etkinin; doğrudan etkilemesidir. Seçmen bazen kitlesel çoğunluğun ağırlıkta olduğu partiye daha meyillidir. Bu durum hem güçlü olan kesim tarafında yer alma hem de nispeten somut beklentilerden kaynaklanabilir. Bazen de seçmen, yakın hissettiği gruba ait oyları parçalamama adına, grubunun favori gösterilen partisini öğrenmek amacıyla da kamuoyu araştırmalarını takip edip etkilenebilir [2]. Fakat toplum zaman zaman anketlerin gerek yanlı davranması gerekse anket sonuçlarının kurcalanarak manipüle edildiği izlenimine kapılarak anketlere karşı güven oluşturamamaktadır. 28 Mart'ta yapılan seçim, 1999 ve özellikle de 2002 genel seçimlerinde büyük sıçrama yapan anketlere olan güveni sarsmış ve onların doğruluklarını şüpheli hale getirmiştir [3].

Kamuoyu araştırmalarında bir veri toplama aracı olarak kullanılan web tabanlı anket metodu, geleneksel anket metodu ile kıyaslandığında, maliyet, zaman ve mesai harcanması açısından

üstündür. Bugün web uygulamalarının hemen hemen hepsi bilgi depolama için veri tabanlarını kullanmaktadır. Web uygulamaları ağırlıkla veri tabanı ile yapısal bir sorgulama dili olan SQL aracılığıyla işlemlerini gerçekleştirir. Saldırgan, veri tabanı hakkında elde ettiği kritik bilgilerle veri tabanında bulunan diğer bilgilere ulaşabilir, bilgileri maniple edebilir. Sonuç olarak saldırganın hedeflediği operasyon başarılı olur [4].

1.1.Blok zincir Teknolojisi

Bloklardan oluşan zincir yapısındaki blok zinciri, şifrelenmiş işlem takibini sağlayan bir veri tabanı sistemi olarak tanımlanabilir. Sistem üzerinde gerçekleştirilen her adım bir blok haline getirilip kendinden önceki blok ile ilişkilendirilir. Gerçekleştirilecek olan işlemler sırasında bloklar şifrelenir, değiştirilemez ve kırılamaz hale getirilir [5,6]. Basit anlamda temel blok zincir yapısı Şekil 1' de gösterilmiştir.



Şekil 1. Blok zincir temel yapısı.

Bilgisayar korsanları birçok farklı yöntemle web sitelerinin tutulduğu sunucu bilgisayarlarına sızabilmekte, veri tabanını ele geçirip kişisel bilgileri elde edebilmekte ya da veri tabanında veriler üzerinde oynamalar yapabilmektedirler []. Blok zinciri, en basit tanımıyla, bir bağlı liste yapısının özelleşmiş halidir. Standart tek bağlı liste yapısında, listenin her elemanı, kendinden sonra gelen elemanı bir işaretçi yordamıyla işaret eder. Bu şekilde listenin başlangıç elemanından kuyruk elemanına kadar bütün elemanlar birbirlerine bağlanmış şekildedirler. Blok zinciri yapısında ise her eleman (blok), sadece sonraki bloğu işaret etmez, aynı zamanda o bloğun öz (hash) değerini de saklar. Diğer bir ifadeyle blok zinciri, özet-işaretçilerle oluşturulmuş özel bir bağlı liste yapısıdır [7].

Blok zincirin, bağlı listeler ile kıyaslandığında öz-işaretçi yapısı açısından elde ettiği en önemli üstünlüğü, liste içerisindeki herhangi bir bloğun değiştirilme durumunda ortaya çıkar. Öz işaretçi yapısı, bu tür bir değişikliğe uğradığında değişiklik yapıldığı rahatlıkla fark edilir. Bunun sebebi yeni eklenen bloğun öz değeri, bu yeni bloğu işaret eden öz işaretçisinin işaret ettiği değerden farklı olacaktır. Bu özellik blok zincirinin güvenli bir yapı olmasını sağlayan en önemli etmendir [8]. Ağda meydana gelen her olay, düğümlerde doğrulanmakta ve kaydedilmektedir. Blok zincirinde ilk başlangıç bloğuna "genesis blok" ismi verilir. Her blok, kendinden önceki bloğun özüt (hash) algoritmasından geçirilmiş içeriğine sahiptir. Böylece sistemdeki bir işlemi değiştirmek isteyen kişi, geriye doğru tüm işlemlerin özüt sonucunu hesaplamak zorundadır. Bu işlem pratik olarak mümkün değildir, çünkü hesaplanan sonuçların tüm madencilerde de aynı olması gerekmektedir [9].

Blok zinciri teknolojisi dağıtık bir defter mimarisi olarak tanımlanabilir. Teorik olarak sistemin defter sayfalarının kullanılması gibi düşünülebilir. Defterin sayfaları defteri kullananlar

tarafından doldurulur. Doldurulan tüm bilgiler defterin önceki sayfalarında silinmeden ve bozulmadan bulunmaya devam eder. Geleneksel defterlerden farklı olarak blok zincirinde her bir sayfa bir sonraki sayfaya şifrelenmiş bir özleme algoritmasıyla bağlanır ve deftere veri akış yönü hep ileri doğrudur [10]. Çalışmanın geri kalan bölümünde sırası ile elektronik oylama sistemleri ile ilgili akademik çalışmalar incelenecek, çalışmada önerilen modelin gerçekleştirilme aşamaları ve algoritmaları açıklanacak ve son olarak önerilen modelin beklenen yaygın etkisinden bahsedilecektir.

2. LİTERATÜR ÇALIŞMASI

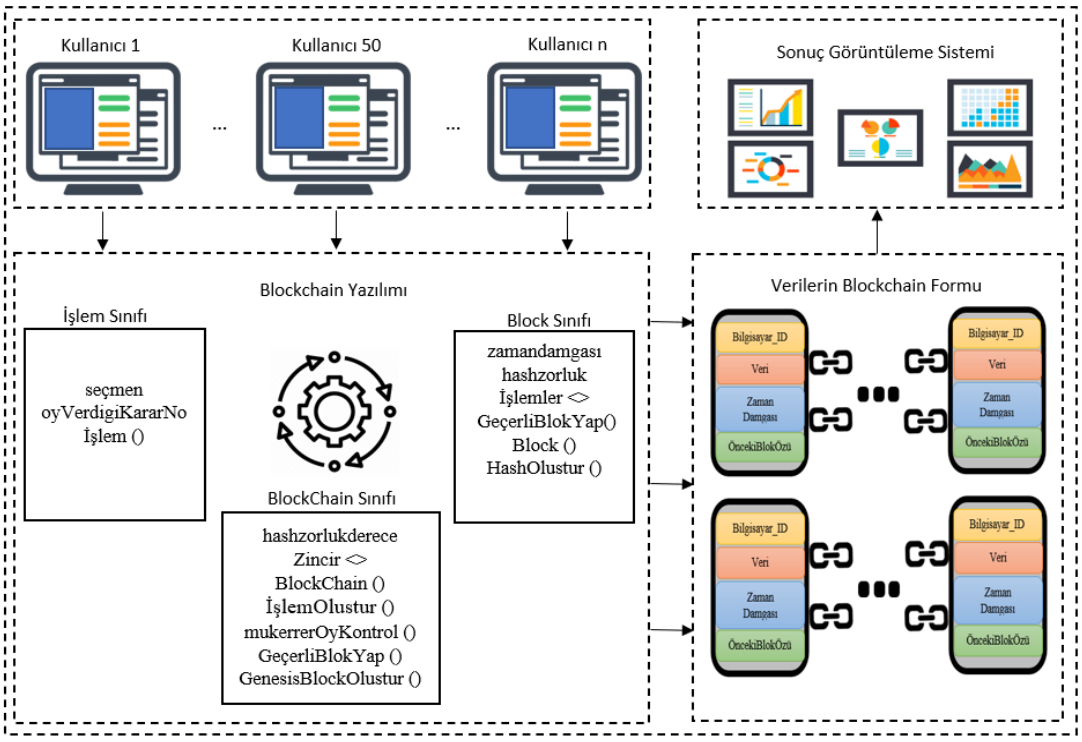
Kohno ve arkadaşları Amerikanın birçok bölgesinde benimsenmiş olan elektronik oylama sisteminin güvenlik açıkları üzerine bir çalışma gerçekleştirmişlerdir. Pazarın önemli bir bölümünde kullanılan bu tür bir makineye kaynak kodunun güvenlik analizini gerçekleştirmişlerdir. Analiz sonucunda, bu oylama sisteminin diğer bağlamlarda geçerli olan en düşük güvenlik standartlarının bile çok altında olduğunu göstermektedir. Yetkisiz ayrıcalık yükseltme, şifrelemenin yanlış kullanımı, ağ tehditlerine karşı zayıflıklar ve kötü yazılım geliştirme süreçleri gibi çeşitli sorunlar tespit edilmiştir. Ayrıca, sisteme düzenlenen ciddi saldırılarda kaynak koduna erişim olmadan bilgilere erişilebildiği gösterilmiştir. Bu tür saldırılar karşısında, içeriden öğrenilen tehditlerle ilgili olağan endişeler tek endişe değildir; yabancılar hasarı yapabilir. Sadece bir anket çalışanı gibi bir içeriden birinin oyları değiştirebileceğini değil, aynı zamanda içerilerin de seçmen mahremiyetini ihlal edebileceğini ve oy kullanan seçmenlerle oyları eşleştirebileceği gösterilmektedir [11]. Bu açıkların tespit edilmesiyle birlikte Kohno ve arkadaşlarının önerdiği model geliştirilerek değiştirilmiş ve güvenlik açıkları kısmen kapatılarak farklı çalışmalar ortaya konmuştur. Clarkson ve arkadaşları Civitas ismini verdikleri, zorlamaya karşı dirençli, evrensel olarak ve seçmen tarafından doğrulanabilen ve uzaktan oylamaya uygun ilk elektronik oylama sistemini oluşturmuşlardır. Sistemlerinin güvenli olduğunu iddia etmelerindeki temel neden kullanıcı doğrulamasını gerçekleştirmeleridir [12]. Çalışmalar güvenlik anlamında başarılı sonuçlar ortaya koydukça maliyet açısından oldukça kazançlı olan bu oylama sistemlerinin kullanımı yaygınlaşmaya başlamıştır. Örneğin Estonya, internet oylamasını ulusal olarak kullanan ilk ülke olmuştur ve bugün oylarının %30'undan fazlası çevrimiçi olarak yayınlanmaktadır [13]. Konuyla ilgili araştırmalar devam ederken, yeni güvenlik konseptlerinden olan blok zincir teknolojisinden yararlanılmaya başlanmıştır. Ayed yeni bir elektronik oylama sistemi için açık kaynaklı blok zincir tabanlı tasarım önermiştir. Önerdiği modelde SHA-256 hash algoritmasını kullanmıştır [14]. Önerdiği model temel blok zincir prensiplerine sahiptir. Önerdiği modelde dezavantaj olarak kullanıcıdan kaynaklı hataların geri döndürülemeyecek şekilde sistemde yer alması gösterilmiştir. Isirova ve arkadaşları blok zincir teknolojisini kullanarak merkezi olmayan bir elektronik oylama sistemi geliştirmek için iki seviyeli yeni konsept önermiştir. Sunulan blok zincir tabanlı oylama protokolünde, oylama şeffaflığı ve anonimlik de dahil olmak üzere bu tür protokollere yönelik tüm gereksinimleri sağlayan altı adımdan bahsedilmektedir. Çalışmada diğer çalışmalardan farklı olarak merkezi güven noktası yoksunluğundan kaynaklı saldırı hedefinden uzaklığı üzerinde durulmuştur [15].

Akademik alanda elektronik oylama sistemleri üzerine yapılan çalışmalar incelendiğinde tespit edilen ve yeni çalışmalara ilham olan ilk zafiyet güvenlik konusudur. Veri güvenliği konusunda yeni bir konsept olan blok zincir yapısı kullanılarak gerçekleştirilen elektronik oylama sistemleri ile bu çalışmada önerilen model arasında benzerlikler bulunmaktadır. Bunlardan bahsedersek kullanılan temel blok zincir esaslarının ve algoritmalarının uygulanması, SHA-256 hash algoritması tercih edilmesi söylenebilir. Mevcut çalışmanın diğer çalışmalarda önerilen

modellerden farkları blok zincire kaydedilen verilerin gösterilme yöntemleri ve aynı cihazdan yalnızca 1 oy kullanabilmeyi sağlayan teknikler olarak söylenebilir.

3. METOD

Bu çalışmada önerilen modelde kullanılan blok zinciri yönetmek için Etheryum, Hyperledger gibi hazır çatılar kullanılmamıştır. C# dili ile uygulamaya özgü blok zincir sınıfları oluşturulup bu yapıyı temel alan güvenli oylama sistemi geliştirilmiştir. Blok zincir sistemini oluşturmak için Block, İşlem ve Blockchain isimli üç ayrı sınıf tanımlanmıştır. Block sınıfı zincirdeki bloklara ilişkin özellik ve metotları içermektedir. İşlem sınıfı zincirde yapılan işlemleri temsil eden nesne yapısını tanımlar. BlockChain sınıfında ise, blok zincirinin yönetimine ilişkin özellik ve metotlar mevcuttur. Bu üç sınıf yapısı aşağıda detaylı biçimde anlatılmaktadır. Geliştirilen yazılımda kullanılan her bir oy bir blok ile temsil edilmektedir. Önerilen modelin mimarisi Şekil 2'de gösterilmektedir.



Şekil 2. Önerilen model mimarisi.

İşlem gerçekleşen her bir oy verme işlemini modelleyen sınıf yapısıdır. İki özellik ve bir kurucu metoda sahiptir. Seçmen, oy kullanılan bilgisayarın ID numarası bu özellikte tutulacaktır. Her bir bilgisayardan sadece 1 oy kullanılabilmesi için mikroişlemci seri numarasından oluşan bir ID numarası kullanılmıştır. oyVerdigiKararNo, seçmenlerin oy verdiği kararın numara bilgisi bu özellikte tutulacaktır. İşlem sınıfının parametreli kurucu metodu kendisine gönderilen bilgileri seçmen ve oyVerdigiKararNo özelliklerine atamaktadır.

Block sınıf yapısındaki özellik ve metodlarını detaylandıracak olursak; zamandamgası, bloğun zincire dahil olduğu tarih/saat bilgisini temsil eder. Hashzorluk özelliği, bir bloğa ait hesaplanan hash değerinin zorluk derecesinin yüksek olması, güvenlik açısından istenen bir durumdur. Block sınıfında bulunan GeçerliBlokYap metodu, hash değerinin ilk iki rakamının 0 olması kuralına uyan hash değerini buluncaya kadar sürekli olarak farklı hash değerleri üreten bir

döngü algoritması içermektedir. Eğer üretilen hash değeri belirtilen zorluk kuralına uymuyorsa başka bir hash değeri üretebilmek için şifrelenecek veri yapısı içinde her adımda değişecek bir veri lazımdır. Bu değişimin sağlanması için bir sayısal değişkenin değeri her denemede 1 artırılmıştır. Örneğin bir bloğa ait üretilen hash değerinin ilk iki rakamı 0 ile başlamıyor kabul edilir ise hashzorluk değişkeni 1 artırılarak tekrar hash değeri hesaplanır ve kurala uyup uymadığına bakılır. Bu şekilde istenen kurala uyan hash değeri hesaplanıncaya kadar hashzorluk değeri 1 artacaktır.

İşlem, blok içerisinde İşlem sınıf yapısındaki elemanlardan oluşan liste yapısıdır. Blok içinde işlem bilgileri bu listede tutulur. Oylama uygulamasında ise kimin hangi karara oy verdiği bilgisi İşlems listesinde tutulacaktır. Hangi seçmenlerin oy kullanıp kullanmadığı, kararların oy miktarları gibi değerlendirmelerin yanı sıra mükerrer oy kullanılmasının önüne geçmek için de İşlems bilgileri kullanılacaktır. ÖncekiBlokÖzü, bir önceki bloğa ait şifrelenmiş özet değerini barındırır. Hash, mevcut bloğa ilişkin şifrelenmiş özet bilgisini barındırır. Bu değer, bir önceki bloğun hash değeri üzerine mevcut blok verisini eklenip tekrar şifrelenmesi sonucu ortaya çıkar.

GeçerliBlokYap metodu, yeni geçerli bloklar oluşturmak için kullanılacak metottur. Metoda gönderilen hashzorlukderece değeri hesaplanacak hash değerinin zorluk derecesini temsil eder. GeçerliBlokYap metodu, hash değerinin ilk birkaç rakamının 0 olması kuralına uyan hash değerini buluncaya kadar sürekli olarak farklı hash değerleri üreten bir döngü algoritması içermektedir. İlk rakamların kaç tanesinin 0 olacağı hashzorlukderece değişkenine gönderilen değerle belirlenir. Eğer üretilen hash değeri belirtilen zorluk kuralına uymuyorsa başka bir hash değeri üretebilmek için tekrar hesaplama yapılır. HashOlustur metodu ile bloktaki zamandamgası, ÖncekiBlokÖzü, İşlemler ve hashzorluk verileri birleştirilerek bir string değer elde edilir. Oluşan string SHA256 (Kriptografik Hash Algoritması) ile şifrelenerek yeni bir hash verisi oluşur. Bu duruma göre bir bloğun hash verisi zaman damgası, bir önceki bloğun hash değeri, işlemler listesi ve hashzorluk değerinin şifrelenmesinden oluşan bir veridir. Ayrıca Block sınıfı kendine gönderilen değerleri sınıf özelliklerine atayan bir kurucu metoda da sahiptir. Hash oluşturma işlemi için uygulanan yöntemin matematiksel modeli Formül 1'de gösterilmiştir.

i: Kayıt indisi,

ZD: Zaman damgası,

YK: Yeni kayıt girişi,

GH: öz çıkarma işlemi,

GAH: Tüm kayıtların özü olmak üzere:

$$YK_i = GH(YK_i + ZD + GAH_{i-1}) \quad (1)$$

BlockChain sınıfı blok zincirinin yönetimine ilişkin özellik ve metotları barındıran sınıftır. Hashzorlukderece zincirdeki blokların sahip olduğu hash değerinin zorluk derecesini temsil eder. Matematiksel modelde yeni kaydın sırasını belirten indis numarası "i" ile gösterilmektedir. "ZD" işlemin gerçekleştirildiği ana ait zaman damgası bilgisini tutan değişkendir. "YK" yeni kayıt oluşturulmasında kullanılan değişkendir. "GH" yeni oluşacak kayıt ile yeni kaydın öncesindeki tü kayıtların ("GAH") birleştirilerek yanlarına zaman damgası ilave edildikten sonra öz işlemini gerçekleştiren fonksiyondur.

Block sınıfı yapısında tanımlanmış "Zincir" ismindeki yapı, zincirdeki blokları içeren ve Block sınıfından elemanlar barındıran listedir. İşlemOlustur metodu yeni bir oy verme işlemi oluşturur. İşlem bilgisini İşlem türünde bir parametre yardımıyla dışardan alır ve işlem bilgisini zincir listesine ekler. GeçerliBlokYap metodu yeni bir blok oluşturur. Şu anki zaman bilgisini ve zincirdeki işlemleri içeren zincir listesini kurucu metod yardımıyla bloğa gönderir. Hashzorlukderece özelliğinde tutulan zincirin zorluk derecesine göre bloğa ait hash bilgisini oluşturur. Zincirdeki en son bloğun hash değerini de blok içerisine dâhil eder. Tüm bunların ardından bloğu zincire ekler. Son olarak da zincirdeki işlem listesini boşaltır. IsValidChain metodu blok zincirindeki blokların kendi hash değerlerinin doğruluğuna bakar. Eğer bir sorun yoksa bloğun kendi içinde barındırdığı önceki bloğun hash verisi ile bir önceki bloğun kendi hash verisini karşılaştıran bir algoritma yardımıyla zincirin doğruluğunu test eder. Kurcalanma tehlikesine karşı zincirin doğruluğunu araştırır. GenesisBlockOlustur metodu genesis bloğu ya da başlangıç bloğu olarak adlandırılan bir blok zincirinin ilk bloğunu oluşturmayı sağlar. MukerrerOyKontrol metodu blok zincirdeki bütün oyları kontrol edilerek bir seçmenin daha önce oy kullanıp kullanmamasına göre true ya da false döndürür. Tekrarlı oy kullanılmasının önüne geçmek için bu metot kullanılmıştır.

3.1. Oy Verme ve Gösterme İşlemi

Seçmen bilgisayarın önerilen model içerisinde yalnızca 1 oy kullanabilme hakkı vardır. Seçmen bilgisayar ID numarası şifreleme işlemine tabi tutularak her bilgisayardan sadece 1 oy kullanılması sağlanmış olunur. Oy verme işlemi esnasında yürütülen algoritma adımları adımlar Tablo 1'de gösterilmiştir.

Tablo 1 Oy verme algoritması

Giriş verileri: Önceki bloğun hash değeri, zaman damgası, işlem verisi, zorluk değişkeni **Çıkış verileri:** Yeni hash değeri
1) Başla 2) Uygulama çalıştırıldığında ağ ortamından blok zincir hesap defterini çek. 3) Mikroişlemci seri numarasını temel alarak benzersiz bir ID numarası üret. 4) Üretilen ID numarasını şifrelenmiş veriye dönüştür. 5) Blok zincirdeki işlem kayıtları kontrol et. 6) Seçmen bilgisayarların ID numaraları ile o anki seçmen bilgisayarın ID numarası karşılaştırılır. 7) Bu bilgisayardan daha önce oy kullanılmışsa oy verme işlemi yapma. 8) Eğer bu bilgisayardan ilk defa oy kullanılıyorsa blok zincirde yeni bir işlem kaydı oluştur. 9) Oy kullanılan bilgisayar ID numarası ve hangi seçime oy verildiği bilgisini kaydet. 10) Önceki bloğun hash değeri, zaman damgası, işlem verisi, zorluk değişkeni verileri kullanılarak yeni bir Hash değeri oluştur. 11) Oluşan Hash değerini yeni bloğun Hash değeri olarak ayarla. 12) Oluşturulan bloğu zincire ekle. 13) Son

Şifreleme işlemi ise hangi seçmenin hangi seçeneğe oy verdiğinin bilinmemesi içindir. Daha sonra bu seçmenin daha önce oy kullanıp kullanmadığı tespit edilmektedir. Eğer ilk defa oy kullanıyorsa blok oluşturulup zincire dahil edilir. Önerilen modele uygulama ara yüzü Şekil 3'de gösterilmektedir.

Şekil 3. Önerilen modelin uygulama ara yüzü.

Blok zincirdeki tüm kayıtlardaki seçmen bilgisi ve oy verdiği karar numarası listelenmektedir. Burada önemli olan seçmen kimlik numaralarının şifrelenmesinden dolayı kimin hangi karara oy verdiğinin anlaşılamamasıdır.

4. SONUÇ

Bu çalışmada, planlanan bir seçim aksiyonunun hızlı, güvenli, şeffaf ve düşük maliyetler ile nasıl gerçekleştirilebileceğine yönelik alternatif bir güvenli elektronik oylama modeli önerilmiştir. Önerilen modelin kullanımı okul, şirket, holding gibi küçük çaplı organizasyonlardan yerel seçimler, genel seçimler, referandumlar gibi büyük çaplı organizasyonalara kadar geniş bir yelpazeye hitap edebilir. Günümüzde küresel bazda yaşanan Covid-19 bulaş hastalığının kalabalık alanlarda yarattığı riskler göz önünde bulundurulduğunda önerilen modelin önemi daha net ortaya çıkmaktadır. Çalışmanın bir sonraki basamağında önerilen modelin web ortamına taşınması ve kimlik doğrulama sistemlerinin mevcut modele entegre edilmesi planlanmaktadır.

KAYNAKLAR

[1] Güz, N., Yanık, H., Yegen, C., Kılıç, I. Ö., & Bingöl, M. (2017). Kamuoyu Araştırmaları ve Medyaya Güven (Credıbılıty Of Publıc Opınıon Surveys And Medıa. Www. Guvenplus. Com. Tr, 1.
[2] Eroğlu, A. H., & Bayraktar, S. (2009). Siyasal Pazarlama Uygulamalarının Seçmen Tercihleri Üzerine Etkileri–İzmir İli Örneği. Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (12), 187-207.
[3] Balcı, Ş., & Ayhan, B. (2004). Seçmen Tercihlerinin Belirlenmesine Yönelik Yapılan Kamuoyu Araştırmalarında Güvenilirlik ve Geçerlilik Problemleri: "28 Mart 2004 Yerel Seçimleriörneği". Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (11), 135-167.
[4] Karakoyun, F., & Kavak, M. T. (2008). Web Anketin Yararları ve Bir Uygulama Örneği Olarak Fizik Tutum Ölçeğine Uygulanması. Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi, (11), 129-141.
[5] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.
[6] Drescher, D. (2017). Blockchain basics (Vol. 276). Berkeley, CA: Apress.
[7] Demirol, D., Daş, R., & Baykara, M. (2013). Sql Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri. In 1st International Symposium On Digital Forensics And Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu) (Pp. 62-66).
[8] Ünsal, E., & Kocaoğlu, Ö. (2018). Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. Avrupa Bilim ve Teknoloji Dergisi, (13), 54-64.
[9] Taş, O., & Kiani, F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine Bir İnceleme. Bilişim Teknolojileri Dergisi, 11(4), 369-382.
[10] Takaoğlu, M., Çağdaş, Ö. Z. E. R., & Parlak, E. (2019). Blokzinciri Teknolojisi Ve Türkiye'deki Muhtemel Uygulanma Alanları. Uluslararası Doğu Anadolu Fen Mühendislik Ve Tasarım Dergisi, 1(2), 260-295.
[11] Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004, May). Analysis of an electronic voting system. In IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004 (pp. 27-40). IEEE.

[12] Clarkson, M. R., Chong, S., & Myers, A. C. (2008, May). Civitas: Toward a secure voting system. In 2008 IEEE Symposium on Security and Privacy (sp 2008) (pp. 354-368). IEEE.
[13] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 703-715).
[14] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 01-09.
[15] Isirova, K., Kiian, A., Rodinko, M., & Kuznetsov, A. Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals.