T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BLOKZİNCİR TABANLI OY VERME SİSTEMİ ÖNERİSİ

Muhammed Emin AYDIN

YÜKSEK LİSANS TEZİ

Endüstri Mühendisliği Ana Bilim Dalı

Kasım - 2018
KONYA

TEZ KABUL VE ONAYI

Muhammed Emin Aydın tarafından hazırlanan “Blokzincir Tabanlı Oy Verme Sistemi Önerisi” adlı tez çalışması 09/11/2018 tarihinde aşağıdaki jüri tarafından oy birliği ile Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Ana Bilim Dalı’nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Prof. Dr. Sabri KOÇER	……..
Danışman Dr. Öğr. Üyesi Ali Osman ÇIBIKDİKEN	……..
Üye Dr. Öğr. Üyesi Muhammed Abdullah BÜLBÜL	……..

Yukarıdaki sonucu onaylarım.

Prof. Dr. Ahmet AVCI
FBE Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz olarak atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

İmza

Muhammed Emin Aydın

09.11.2018

ÖZET

YÜKSEK LİSANS TEZİ

BLOKZİNCİR TABANLI OY VERME SİSTEMİ ÖNERİSİ

Muhammed Emin AYDIN

Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü
Endüstri Mühendisliği Ana Bilim Dalı

Danışman: Dr. Öğr. Üyesi Ali Osman ÇIBIKDİKEN

2018, 54 Sayfa

Jüri
Dr. Öğr. Üyesi Ali Osman ÇIBIKDİKEN
Prof. Dr. Sabri KOÇER
Dr. Öğr. Üyesi Muhammed Abdullah BÜLBÜL

Online seçim sistemlerinin sunduğu avantajlar göz önüne alındığında, güvenli bir online seçim sisteminin yapılabilmesi birçok ülke ve organizasyon için çok önemlidir. Bu seçim sistemlerini kökünden değiştirebilecek ve hatta demokrasinin gelişmesine katkıda bulunabilecek bir yaklaşımdır. Blokzinciri tabanlı günümüze kadar öne sürülmüş seçim sistemlerini incelenerek, bunların avantajları ve dezavantajları ortaya koyulmuştur. Pratikte kullanılabilecek bir oy verme sistemin genel yapısı çıkarılmıştır. Ayrıca önerilen sistemin çalışan bir modeli uygulama olarak geliştirilmiştir.

Anahtar Kelimeler: Blokzinciri, dağıtık sistem, kripto para, seçim sistemi, online seçim sistemi

ABSTRACT

MS THESIS

BLOCKCHAIN BASED VOTING SYSTEM PROPOSAL

Muhammed Emin AYDIN

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF NECMETTIN ERBAKAN UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE
IN INDUSTRIAL ENGINEERING

Advisor: Assistant Prof. Dr. Ali Osman ÇIBIKDİKEN

2018, 54 Pages

Jury
Assistant Prof. Dr. Ali Osman ÇIBIKDİKEN
Prof. Dr. Sabri KOÇER
Assistant Prof. Dr. Muhammed Abdullah BÜLBÜL

Given the advantages offered by online selection systems, the ability to make a secure online selection system is very important for many countries and organizations. This is an approach that can change the electoral system from the root and even contribute to the development of democracy. The advantages and disadvantages of the election systems that have been put forward as much as the day-to-day problems of blockchain are examined. The general structure of a voting system that can be used in practice has been removed. In addition, a working model of the proposed system has been developed as an application.

Keywords: Blockchain, distributed system, crypto currency, voting system, online voting system

ÖNSÖZ

Tez çalışmam sırasında yaptığı katkılar ve desteklerden dolayı danışmanım Necmettin Erbakan Üniversitesi Bilgisayar Mühendisliği öğretim üyesi Dr. Öğr. Üyesi Ali Osman Çıbıkdiken'e teşekkür ederim.

Muhammed Emin AYDIN
KONYA - 2018

İÇİNDEKİLER

1. GİRİŞ

Günümüzde seçim sistemleri uzun yıllardan beri alışılagelmiş şekilde oldukça fiziksel ve ilkel yöntemlerle yapılmaktadır. Teknolojik gelişmeler seçim sistemlerinde pek bir değişikliğe sebep olmamıştır. Bunun sebebi teknoloji kullanılarak yapılan çözümleri klasik sistemden daha az güvenli olması ve hile yapılmasına daha açık olmasıdır.

Oylama sistemleri online ortama taşınabilir ise, klasik seçim sistemlerine kıyasla çok daha düşük bir maliyetle yapılabilir. Ayrıca oylama konusunda da çeşitli kolaylıklar sağlayacaktır.

Bir online oylama sisteminin iki önemli problemi vardır. Birincisi böyle bir sistemin güvenliğini sağlamak ve kayıtların kesinlikle değiştirilmediğine emin olmak çok zor bir iştir. İkincisi oy kullanan kişilerin kimlikleri kesinlikle gizli olmalıdır. Bunu online sistem üzerinde sağlamak çok zor bir iştir.

Son yıllarda kripto paralar sayesinde isminden sıkça bahsedilen **blokzinciri** (*blockchain*) teknolojisi bu problemleri çözebilir. Blokzinciri; hiçbir merkezi noktadan yönetilmeyen, ağda bulunan üyelerin birbirlerine güvenmelerini gerektirmeyen, içerisindeki verilerin kimse tarafından değiştirilemeyeceği şeffaf ve dağıtık veri depolama ile ortak bir noktada fikir birliğine ulaşma sistemidir. İlk olarak Bitcoin adındaki elektronik para biriminde kullanılmak amacı ile geliştirilmiştir. Ancak daha sonra farklı amaçlarla da kullanılabileceği ortaya konulmuştur. Bu alanlardan birisi de oylama sistemidir.

Blokzinciri teknolojisi bir online seçim sisteminin sahip olması gereken bazı güvenlik özelliklerini sağlasa da çok şeffaf bir yapıya sahip olduğu için ekstra güvenlik protokolleri ile desteklenmesi gerekir. Bu sayede oyların gizliliği ve seçmenin güvenliği sağlanmış olur. Blokzinciri teknolojisinin çok daha öncesinden itibaren kriptoloji yardımıyla seçim sistemi çalışmaları yapılmıştır. Bu çalışmalar ile blokzincir teknolojisi bir araya getirilerek gerçek manada güvenli bir seçim sistemi elde edilebilir.

1.1. Çalışmanın Amacı

Blokzinciri tabanlı günümüze kadar öne sürülmüş seçim sistemlerini incelemek, bunların avantajlarını ve dezavantajlarını ortaya koymak ve pratikte kullanılabilecek bir sistemin genel yapısını çıkarmak bu çalışmanın temel amacını oluşturmaktadır.

Konunun teorik zeminin verdiği alt yapı ile pratik bir uygulamasının detayları verilmiştir. Böylece pratikte kullanılabilecek yeni bir yöntem oluşturulması amaçlanmıştır.

1.2. Çalışmanın Önemi

Online seçim sistemlerinin sunduğu avantajlar göz önüne alındığında, güvenli bir online seçim sisteminin yapılabilmesi birçok ülke ve organizasyon için çok önemlidir. Bu seçim sistemlerini kökünden değiştirebilecek ve hatta demokrasinin gelişmesine katkıda bulunabilecek bir çalışmadır.

1.3. Tezin Yapısı

Tez dört bölümden oluşmaktadır.

İkinci bölümde online seçim sistemleri araştırılmıştır. Bu alanda yapılmış çalışmalar incelenerek, böyle bir sistemin avantajları ve dezavantajları verilmiştir. Ayrıca blokzinciri teknolojisi ele alınmıştır. Bu teknolojinin bir seçim sistemine nasıl bir katkı sağlayabileceği ortaya konmuştur.

Üçüncü bölümde online bir seçim sisteminin güvenliğini sağlamak için blokzinciri teknolojisine eklenebilecek kriptolojik protokoller ve yöntemler incelenmiştir.

Dördüncü bölümde ise pratikte kullanılabilecek bir seçim sistemi oluşturulmaya çalışılmış ve bunun uygulaması geliştirilmiştir.

Beşinci bölümde önerilen seçim sistemi için sonuçlar değerlendirilmiştir. Ayrıca gelecek çalışmalar hakkında bilgi verilmiştir.

2. KAYNAK ARAŞTIRMASI

2.1. Online Seçim Sistemi

Teknolojinin gelişmesi ile günlük hayatımızdaki her şey teknoloji kullanılarak daha kolay ve hızlı hale gelmektedir. Ama dünya üzerinde seçim sistemleri ve oylama sistemlerine bakılırsa bu konuda ciddi bir eksiklik söz konusudur. Dünya genelinde (özellikle batıda), vatandaşların seçimlere gösterdiği ilgi her geçen gün azalıyor. Seyahat sağlık gibi sebeplerden dolayı insanlar sandığa gitmekte zorlanıyorlar. Bu alanda sunulacak teknolojik kolaylıklar seçime olan katılımı da artıracaktır. Estonya dışında hiçbir ülke tam olarak online seçim sistemini kullanmamaktadır. Bunun sebebi tam olarak güvenli bir online seçim sistemi geliştirmenin imkansıza yakın derecede zor olmasıdır. Estonya'nın bunu başarmış olması aslında Estonya nüfusunun azlığı ve ülke içindeki çekişmenin sorun çıkaracak seviyede olmamasıdır. Bu sayede belli bir merkezi konuma insanlar güvenmektir. Buna rağmen 2014 yılında yayımlanan bağımsız bir raporda Estonya daki seçim sisteminin aslında çok da güvenli olmadığı ortaya konulmuştur. Ayrıca diğer bazı ülkelerde kullanılan elektronik oy kullanma makinelerinin güvenliği ise sürekli olarak tartışılmaktadır.

Yaklaşık 30 yıldır bir çok ülkede e-oylama konusu tartışılmış ve çeşitli şekillerde yasalara girmiştir. Fakat çok az ülke bunları gerçek hayatta kullanmaktadır. Bunun en büyük sebebi güvenlik endişeleri ve uygulama zorluklarıdır. Oy kullanma makineleri ise bazı ülkelerde kullanılmaktadır. Fakat oy kullanma makinelerinin güvenliği ile ilgili endişeler bir çok yerde ortaya konulmuştur (Hao ve Ryan, 2016).

İngiltere’de artan taleplere rağmen online oylamanın güvenliği ile ilgili olan endişeler sebebiyle gerçek manada hiçbir adım atılmamıştır (Kettley, 2017).

2012 yılında, Fransa’da yetkililer, yurtdışında yaşayan vatandaşları için bir online oylama web portalı kurmuştur. Bu sistem bir özel şirket tarafından geliştirilmiştir (Scytl Online Voting, 2015). Bu uygulama siber saldırı endişeleri göz önüne alınarak kaldırılmıştır (Pennetier ve ark., 2017).

Bazı ülkeler elektronik oy kullanma makinelerini bir süre kullanmış ama bazı tartışmalardan dolayı daha sonra bırakmışlardır. Mesela Hollanda bu ülkelerden biridir (Lowe, 2017).

Sonuç olarak merkezi bir konuma güven gerektirmeden güvenli bir online seçim sistemi geliştirmek çok zor bir iştir. İşte tam bu noktada blokzincir teknolojisi ön plana çıkmaktadır. Çünkü blokzincir merkezi güven noktasını ortadan kaldırmaktadır.

Seçmenin verdiği oyu güvenilir bir algoritma ile sisteme aktarabilecek bir yapı aynı zamanda temsili demokrasi ile doğrudan demokrasi arasındaki aşılmaz olarak görülen uçurumuda bir ölçüde kapatmaya yardımcı olabilir. Bu sayede blokzincir teknolojisi seçim sisteminin yanı sıra yasama sürecinin evrilmesi anlamında da bir rol üstlenebilir.

Online seçim sistemlerinde ayrıca elektronik oy verme de kullanılabilir. Elektronik oy verme oy kullanımının makinelerle yapıldığı sistemdir. Oyunu web sitesi üzerinden kullanmak istemeyenler seçim merkezlerine gidip oy makinelerini ve kimlik kartlarını kullanarak oy verebilirler.

2.1.1. Online seçim sisteminin faydaları

Online seçim sistemleri pek çok açıdan fayda sağlamaktadır. Bunları başlıca şu şekilde sıralayabiliriz.

a) Maliyet

   Online seçim sistemleri klasik seçim sistemlerine nazaran çok daha düşük bir maliyetle gerçekleştirilebilir oy sandıkları gözetmenler seçimini yapıldığı binalar ve bunların hepsinin maliyetleri göz önüne alınacak olursa online seçim sistemlerinin çok daha ucuza mal edilebileceği görülecektir**,**

b) Hazırlık süresinin kısalığı

   Klasik seçim sisteminde aylar öncesinden hazırlık yapılması gerekmektedir. Ama bu süre online seçim sistemlerinde çok kısadır. İsviçre gibi yılda defalarca referandum yapan direkt demokrasi uygulanan ülkelerde online seçim sistemlerinin ne kadar kolaylık sağlayacağı ortadadır. Hatta her hafta referandum yapmak bile mümkündür

c) Oy kullanma rahatlığı

   Online seçim sisteminde oy kullanan kişiler istedikleri her yerden rahatlıkla oy

kullanabilirler. Bu da insanların herhangi bir konuma bağlamaz. Bu sayede dünyanın her yerinden oy kullanabilirler. Büyükelçiliklerde ve havalimanlarında oy kullanılmasına gerek kalmaz,

d) Hız

Online seçim sisteminde sayım bilgisayar ortamında yapıldığı için ve fiziksel herhangi bir sayım olmadığı için sonuçlar çok hızlı bir şekilde belli olmaktadır.

e) Farklı oylama sistemlerini mümkün kılması

Klasik seçim sistemlerinde sadece bir tercih yapılabilir. Ama online seçim sistemlerinde çok farklı oylama sistemleri uygulanabilir. Mesela birden fazla seçeneğin seçilebilmesi veya seçeneklere puanlandırma yapılabilmesi sağlanabilir. Bu sayede çok farklı referandumlar yapılabilir. bu teknoloji sayesinde, çok-boyutlu oy kullanma (politika bazlı parti destekleme) imkanı da ihtimaller arasında. Seçimler, toptancı bir oylama yöntemi ile değil, politika tipleri çerçevesinde yapılabilir. Seçmenler, oy verme işleminin maliyetinin azaltıldığı bir sistem içerisinde, A partisini sağlık politikası, B partisini eğitim politikası, C partisini de ekonomi politikası uygulamak için seçebilir.

2.1.2. Bir seçim sisteminin güvenliği

Öncelikle online veya offline bir seçim sisteminin sahip olması gereken özellikleri inceleyeceğiz. İlerleyen bölümlerde bu maddelerin burada önerdiğimiz online seçim sistemiyle uyuşup uyuşmadığı incelenecektir.

Bir seçim sisteminin sahip olması gereken temel özellikler şu şekilde belirlenebilir:

a) Seçmenlerin kimliği tamamen gizli tutulmalıdır.

Doğru işleyen demokraside seçmenlerin oy kullanırken ne yönde oy kullandıkları tamamen gizli olmalıdır. Bu sayede insanlar özgür bir şekilde seçimlerini yapabilirler. Eğer bu özgürlük olmazsa seçim sisteminin bir manası kalmaz.

b) Sadece oy kullanma hakkı olan kişiler oy kullanabilmeli

Bir seçim sisteminde oy kullanılabilecek kişiler bellidir. Bu kişiler dışında kimse

oy kullanmamalıdır. Yani sistemde sahte oy olmamalıdır. Kişilerin kimliklerinin gizli olması gerektiğini de göz önüne alırsak online sistemlerde bunu yapmak zordur. Klasik seçim sistemlerinde bu seçmen listesi ve kimlik kontrolü ile sağlanabilir. Oy kullanımı fiziksel olarak gizli olduğu için bir sıkıntı oluşturmaz. Online seçim sistemlerinde kriptolojik protokoller kullanarak bu problem aşılabilir.

c) Her seçmen sadece bir kere oy kullanabilmelidir.

   Düzgün bir seçim yapılabilmesi için ve oy sayımının doğru olması için her seçmen yalnızca bir oy kullanabilmelidir. Oy kullananların kimliğinin gizli tutulması online seçim sistemlerinde sorun teşkil etmektedir. Genellikle bunu açabilmek için üçüncü bir yetkilendirme sunucusu kullanılmaktadır. Bu yöntem başka sıkıntılarda ortaya çıkarabilir. Bunlar ilerleyen bölümlerde incelenecektir.

d) Oyların sayımının doğrulanabilir olmalıdır.

   Bir seçim sisteminde kullanılan oyların doğru sayıldığı, bir otoriteye güvenmeyi gerektirmeden doğrulanabilmelidir. Bu isteyen herkes tarafından yapılabilmelidir. Klasik seçim sistemlerinde bu durum seçime katılan tarafların yaptığı gözetmenlik sayesinde mümkün olmaktadır. Online sistemlerde bu durum daha fazla halka açık bir şekilde yapılmalıdır. Bu sayede daha güvenli olacaktır. blokzincir teknolojisinin önemi bu noktada daha fazla ön plana çıkmaktadır.

e) Bireysel olarak oylar doğrulanabilir olmalıdır.

   Online seçim sistemlerinde oy kullanan bireylerin kullandıkları oyları değiştirilmediğinden emin olabilmeleri gerekir. Klasik seçim sistemlerinde bu gerekli değildir. Çünkü kullanılan oyun güvenliği fiziksel olarak sağlanmıştır. Online sistemlerde bunu sağlamak için ekstra yöntemler kullanılması gerekir.

f) Baskı altında oy kullanılmamalı ve oyların satılamamalıdır.

   Klasik seçim sisteminde oy kullanımı kapalı bir kabin içerisinde diğer insanlardan uzak olarak gerçekleştiği için özgür irade ile oy kullanılmaktadır. Online seçim sistemlerinde insanların evlerinde dahi oy kullanabilmesi amaçlandığından dolayı baskı altında oy vermesi mümkün olmaktadır. Bu durum insanların oylarını seçim süresi dolmadan değiştirebilmeleri sağlanarak kısmen

çözülebilir. Ayrıca kullanılan oylar daha sonra doğrulanabildiği için oyların satılabilmesi de mümkündür. Çünkü verilen oyu doğrulamak için kullanılan sistem, başkalarına verilen oyu ispatlamak için de kullanılabilir. Bu sayede verilen oy karşılığında maddi bir karşılık istenebilir. Bu da düzgün işleyen bir demokraside olmaması gereken bir durumdur. Bu durumu engellemek amacıyla oyu doğrulamak amacıyla verilen referans bilgisi kolay elde edilebilen bir bilgi olursa oyların satılabilirliği azaltılmış olur. Ama bu durumla ilgili kesin bir çözüm bulunmamaktadır. Bu konuda daha fazla çalışma yapılması gerektiği ortadadır.

2.2. Blokzinciri Teknolojisi

Blokzinciri (*Blockchain*) teknolojisi; ilk olarak Bitcoin adındaki, yazılımsal bir para birimi için, 2009 yılında, takma isimle yayınlanmış bir makale ile ortaya konulmuş bir teknolojidir (Nakamoto, 2009). Sistemde adresler arasındaki para aktarımı tamamiyle herhangi bir merkeze bağlı olmadan dağıtık bir şekilde çalışan sistemler aracılığıyla yürütülmektedir. blokzincir teknolojisi kripto paralar adı verilen yeni bir finansal aracın ortaya çıkmasını sağlamıştır. Blokzincir teknolojsi birçok uzmana göre internetten sonra dünyadaki birçok sektörü değiştirebilecek en önemli gelişmedir. Verilerin açık olması ve değiştirilemez olması blokzincir teknolojisinin en önemli özelliğidir. Blokzincir kripto paralar dışında birçok amaçla kullanılabilir. Bunlar genellikle merkezi bir güven noktasının olmaması gereken işlerdir. Online seçim sistemleri ise bunun için en güzel örnektir.

Szabo (1997), tarafından yayınlanan makalede Bitcoin’den önce herhangi bir merkezi olmayan, genele açık network uygulamalarının uygulanabilmesi için çeşitli yöntemleri ortaya koymuştur.

Courtois (2014) makalesinde, en temel blokzincir algoritmalarını ve onların güvenliğini incelemiştir.

Evans (2014) çalışmasında Bitcoin’i bir para birimi olarak ekonomik ve sosyolojik açıdan incelemiştir.

Bitcoin yaygınlaşmaya başladıktan sonra, Bitcoin protokolünün iyileştirilmesi için çeşitli araştırmalar yapılmış ve yeni algoritmalar geliştirilmiştir. Bu algoritmalar hakkında bir çok makale yayınlanmıştır. Mesela Proof-of-Work algoritmasına alternatif olarak Proof-of-Stake algoritması geliştirilmiştir. Proof-of-Stake hakkındaki ilk makale King ve Nadal (2012) tarafından, yayınlanmıştır. BitFury Group (2015) tarafından, Proof-of-Stake algoritmalarının genel incelemesinin yapıldığı bir çalışma yayınlanmıştır.

Bitcoin'in uygulama alanlarını çoğaltmak amacıyla, Payment Channels, Lightning Network, Merkle Tree, Impusle gibi algoritmaları geliştirilmiş ve bunlar hakkında makaleler yayınlanmıştır.

Poon ve Dryja (2015) makalesinde, Lightning Network algoritmasıyla kişiler arasında masrafsız ödeme kanallarının kriptolojik yöntemlerle nasıl oluşturulabileceğini incelemişlerdir.

Todd (2014) çalışmasında masrafsız ödeme sistemini incelemiştir ve yeni algoritma önerilerinde bulunmuştur.

Decker ve Wattenhofer (2014) makalesinde kriptolojik ödeme kanallarını incelemişlerdir.

Sompolinsky ve Zohar (2014), Blokzincir ve Bitcoin’in kullanıcı sayısının artmasıyla ortaya çıkabilecek performans problemlerini incelemiş ve çeşitli çözüm önerileri sunmuşlardır.

BitPay şirketi (2015) Impusle adı verilen yeni bir ödeme kanalı teknolojisini sektöre tanıtmıştır.

Blokzincir teknolojisinin Bitcoin dışında daha farklı uygulamalara da uygulanabilmesi, daha genel ve programlanabilir bir hale getirilebilmesi için yeni fikirler ortaya atılmıştır. Bunlar önce alternatif para birimleri oluşturmak için ortaya atılmış color coin, sidechain, treechain gibi algoritmalardır.

Back ve ark. (2014) bir makale yayınlanmış ve bu makalede ana bir blokzincire bağlantılı birden fazla blokzincirin nasıl oluşturulabileceğini ve bu zincirler arasındaki iletişimin ve güvenliğin nasıl olabileceğini incelemişlerdir.

Daha sonra programlanabilir blokzincir fikri daha da geliştirilerek programlanabilir akıllı sözleşmelere ve programlanabilir para birimlerine kadar gelmiştir.

Bu projede kullanılacak olan programlanabilir blokzincir teknolojisine örnek olarak Ethereum, Bitshares, CounterParty, MasterCoin, NXT ve DASH gibi teknolojiler örnek gösterilebilir. Bu sistemlerin algoritmaları ile ilgili çeşitli makaleler yazılmıştır.

Buterin (2014) makalesinde Ethereum platformu hakkında bilgi vermiş ve akıllı sözleşme programlama modelini tanımlamıştır.

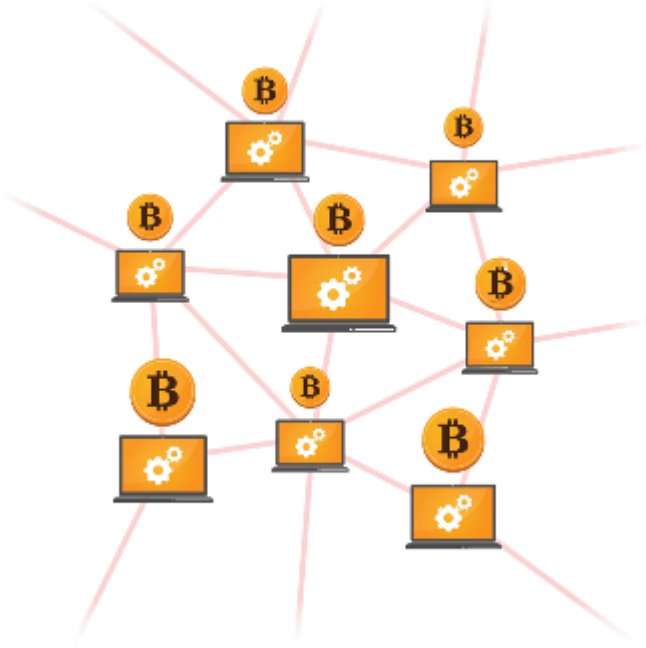
Wood (2015) Ethereum platformunda transaction'ların kullandığı algoritmaları anlatmıştır.

2.2.1. İlk Blokzincir: Bitcoin

Bitcoin 2009 yılında ortaya çıkmış internet üzerinde bulunan bir para sistemidir. En önemli özelliği herhangi bir Merkezi yönetime sahip olmamasıdır. Bu teknolojiyi ilk ortaya atan kişi kimliği bilinmeyen bir kişidir. Çünkü birçok ülkede alternatif para birimi oluşturmak suç sayılabileceği için, bitcoin fikrini ortaya atan kişi kimliğini gizlemiştir. Ama Bitcoin Protokolü ve yazılımın kodları tamamen açıktır ve şu anda dünya genelinde gönüllü programcılar tarafından geliştirilmektedir.

Bitcoin'in bütün para politikası tamamen açıktır ve değişken değildir. Mesela toplamda oluşacak olan Bitcoin sayısı bellidir ve değiştirilemez ve yavaş yavaş üretilmektedir. Bitcoin'ler belli bir merkezden dağıtılmamaktadır (Şekil 2.1.). Yeni bitcoin'leri üreten bitcoin madencileri bulunmaktadır. Herkes madenci olabilir. Çünkü belli bir merkezden yönetilmemektedir. Aslında madenciler bir yazılım kullanılarak güçlü bilgisayarlar yardımıyla belli matematiksel işlemler yaparak yeni bitcoin'leri elde etmeye çalışmaktadırlar. Bu işlem çok fazla işlem gücü ve elektrik gerektirmektedir. Bitcoin madenciliği ciddi bir rekabet içeren sektördür. Bütün madenciler yeni üretilecek bitcoin'leri ele geçirmek için sürekli daha fazla yatırım yaparlar ve ellerindeki hesaplama gücünü artırmaya çalışırlar. Bu aynı zamanda Bitcoin sisteminin güvenliğini sağlar. Bu sayede Bitcoin üzerinde kaydı tutulan işlemler değiştirilemez. Bitcoin'in para politikası matematiksel ve yazılımsal olarak sabittir. Mesela toplamda sadece 21

milyon Bitcoin oluşacaktır ve bundan daha fazla Bitcoin üretilmeyecektir. Şu ana kadar yaklaşık 16 milyon bitcoin üretilmiştir ve üretimi gittikçe yavaşlamaktadır ve 2140 yılında üretiminin biteceği hesaplanmaktadır.



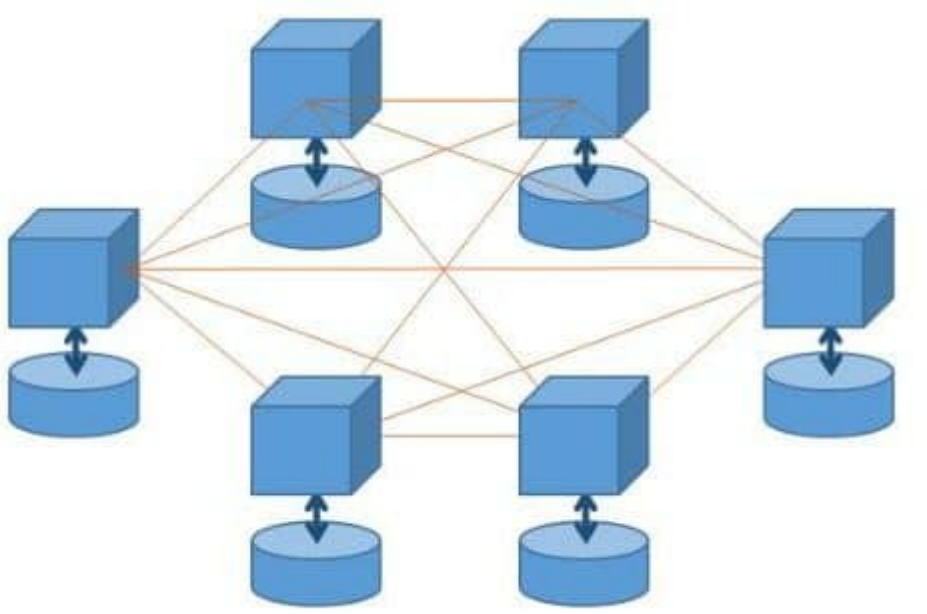
Şekil 2.1. Bitcoin'in blokzinciri içerisinde düğüm noktalarına bağlı yapısı

Bitcoin yönetim biçimi bakımından internete benzetilebilir. Daha çok kişiden kişiye yani uçtan uca para transferini mümkün kılar. Herhangi bir banka veya benzeri bir kuruluşa ihtiyaç yoktur. Bu özelliği ile nakit paraya da benzemektedir.

2.2.2. Blokzinciri Nedir?

Blokzinciri aslında bir kayıt defteridir. Herkese açık, şeffaf, dağıtık, sıralı ve zaman damgalı verileri içeren dijital küresel bir kayıt defteridir. Düz bir veri dosyası, basit bir veritabanıdır (Şekil 2.2.). Bu deftere sadece kayıt eklenebilir ama kayıt silinemez veya değiştirilemez. Blokzincir üzerindeki kayıtlar birbirleri ile rekabet halinde olan tarafların oluşturduğu bloklardan oluşmaktadır. Aslında sahip olduğu güvenliği bu rekabet unsurundan almaktadır. Bir blokzincir ağında bulunan her bir

katılımcıya genelde madenci denilmektedir. Bunun sebebi bu kavramların genelde Bitcoin'den gelmiş olmasıdır. Bitcoin ağındaki katılımcılar madenci olarak adlandırılır.



Şekil 2.2. Blokzincirinin dağıtık veritabanı gösterimi.

Blokzincir üzerinde veriler merkezi olmayan bir ağ yapısındaki uç bilgisayarlarda, birbirinden bağımsız olarak saklandığından, herhangi bir merkezi hatadan kaynaklanabilecek problemlere karşı dirençlidir. Bu ağda bulunan her bilgisayar aslında bu blokzincirine ait bütün işlemleri yani bütün geçmişi kendi üzerinde tutar. Bu nedenle aslında verilerin her bilgisayarda bir kopyası tutulmuş olur. Mesela Bitcoin ağı üzerinde şu anda yüzlerce gigabyte'lık bir veri bütün Bitcoin node'ları tarafından tutulmaktadır. Bu nedenle geçmişi değiştiremezsiniz.

Ayrıca blokzincir üzerindeki geçmiş bilgilerin değiştirilememesi rekabete dayalı madencilik algoritmaları sayesinde sağlanır. Çünkü bu rekabet sayesinde blok zinciri hep ileriye doğru ilerler. Hiç durmaz veya gerilemez. Çünkü blokzincir kuralları gereği en uzun zincir doğru zincirdir. Bu rekabet ortamı bir blokzincir'in güvenliği için en önemli unsurdur.

2.2.3. Blokzinciri teknolojisinin temel özellikleri

a) **Herkese açık bir veri tabanıdır:**

Blokzincir teknolojisi kısıtlanmadığı takdirde herkese açık bir veritabanıdır. Herkes istediği zaman bağlanıp sisteme veri girebilir ve işlem yapabilir. Fakat bazı durumlarda bu erişimin kısıtlı olması istenebilir. Mesela online seçim sistemi için kullanılıyorsa sadece oy kullanabilecek kişiler işlem yapabilir ve sadece yetkili taraflar madencilik yapabilir.

b) **Şeffaflık:**

Blokzincir üzerinde bulunan bütün bilgiler herkes tarafından görülebilir ve incelenebilir. Çünkü bütün kayıtların bütün madencilerde ve talep eden kişilerde kopyası bulunmaktadır. Blokzincir üzerindeki bir bilgi gizlenmek isteniyorsa şifrelenmiş bir şekilde blokchaine konulmalıdır. Mesela online seçim sisteminde oyların gizli olması isteniyorsa, ya oylar şifrelenerek blokchaine yazılır yada oyun ait olduğu kişi gizlenerek yazılır.

c) **Dağıtık bir sistemdir:**

Blokzincir merkezi bir noktası bulunmayan bir ağdır. Bu ağdaki bütün katılımcılar ağın sahip olduğu protokol kurallarına uydukları sürece eşit şartlarda çalışırlar. Ağda bulunan uç noktalarda bir ya da birkaçının hile yapması veya kaybolması ağın işleyişini etkilemez. Eğer ağın çoğunluğu protokol kurallarına uyarsa hiçbir şekilde hile yapılamaz veya birkaç sunucu ayakta kalsa bile ağ çalışmaya devam eder.

d) **Veriler sıralıdır ve zaman damgalıdır**:

Blokzincir üzerindeki kayıtlı veriler sıralı ve birbirine bağlıdırlar ve genellikle kaydedildikleri zamanı içeren bir zaman damgasına sahiptirler. Blokzincir üzerinde bulunan verilerin sırası değiştirilemez. Veya aradaki verilerde değişiklik yapılamaz. Bu blokzincirin bütünlüğünü bozar. Çünkü her biri kendinden önceki veriye bağlı olarak işlenmiştir. Blokzincir ismi buradan gelmektedir. Blok zincirler halinde kaydedilirler ve bir tane zincir halkasını dahi aradan çıkaramazsınız.

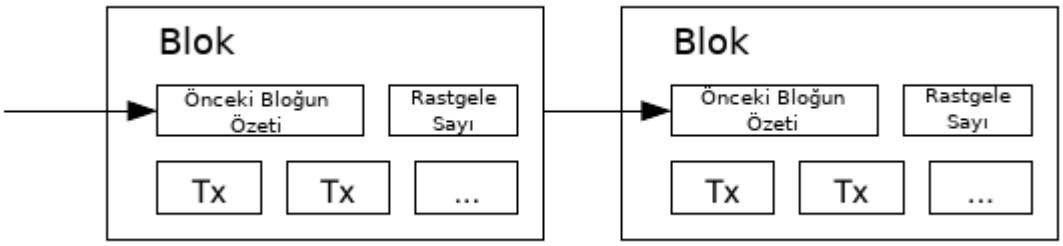
e) **Bilgiler değiştirilemez:**

Kaydedilen bilgiler bütün madenciler anlaşmadığı sürece silinemez. Hatta böyle bir durum olduğunda dahi eski zincir herhangi bir kişide bulunuyorsa silmeye çalışılan bu bilgilerin varlığı kanıtlanabilir. Ayrıca madencilerin kendi arasında rekabet ettiği de düşünülecek olursa verilerin silinmesi pratikte imkânsızdır. Ayrıca bir verinin değiştirilmesi bütün blockchanin kriptolojik olarak bütünlüğünü bozar.

2.2.4. Blokzinciri veri yapısı

Blokzincir üzerinde kayıtlı her işlem transaction olarak adlandırılır. Transactionlar bir araya gelerek blokları oluştururlar. Bloklar ise birbirine bağlanarak bir zincir oluşturulmuş olur. Genellikle transactionlar içerisinde bir dijital imza barındırırlar. Bu imza o transaction in kabul edilebilir olması için gerekli özelliktir. Mesela bitcoin üzerinde bir para gönderme işlemi o paraya sahip olan kişinin dijital imzası ile imzalanmaktadır.

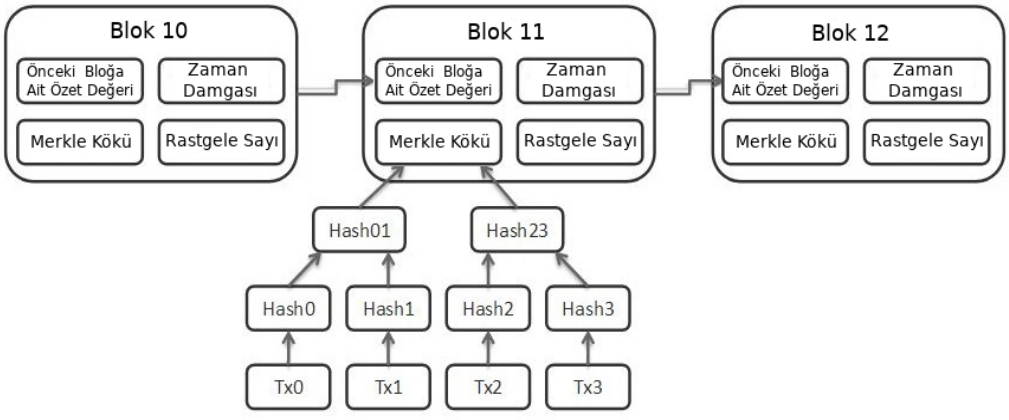
Bir online seçim sisteminde ise bu dijital imza o transaction içerisinde bulunan oyun yetkilendirme otoritesi tarafından onaylandığını belirten bir dijital imza içermelidir. Transactionlar madenciler tarafından toplanır ve protokolde belirtilen aralıklarla bir blok haline getirilir. Mesela belirlenen blok süresi 1 dakika ise 1 dakika boyunca toplanan transactionlar bir araya getirilerek bir blok oluştururlar. Bu süreç aslında sabit bir süre değildir. Olasılıksal olarak değişiklik gösterir. Mesela bitcoin de 1 blok bulunması bir hesaplama işlemine bağlı olduğu için ortalama olarak her 10 dakikada bir blok bulunur. Ama bu ortalama bir değerdir. Gerçek hayatta sürekli değişiklik göstermektedir. Belli zaman aralıklarında üretilen bu bloklar kendilerinden bir önceki bloğun hash değerini içerirler. Bu sayede her blok kendinden bir önceki bloğa bağlanmış olur (Şekil 2.3.).



Şekil 2.3. Blokzinciri içerisinde blokların birbirine bağlanması.

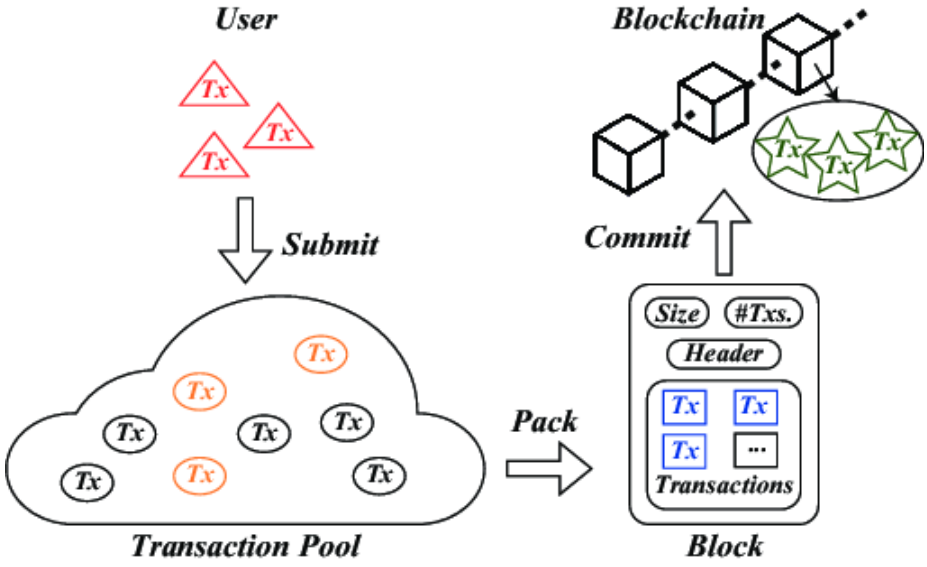
Hash fonksiyonu kendisine verilen herhangi bir uzunluktaki veriyi alıp kısa ve sabit bir uzunlukta özet bilgi üreten bir fonksiyondur. Aynı girdi olduğu müddetçe her zaman aynı sonuç çıkacaktır. Ama veri içerisinde en ufak bir değişiklik olursa çıkan sonuç tamamiyle farklı olur. Bu sayede bir verinin değişip değişmediğini anlamak için hash fonksiyonundan çıkan özet değere bakılabilir.

Her blok içerisinde bulunan transactionlar Merkle tree denilen bir ağaç veri yapısında tutularak ağacın kök değeri blog başlığına yazılır (Şekil 2.4.). Bu transactionlarda herhangi birisinde en ufak bir değişiklik olursa bu ağacının kök değeri değişecektir. Bu sayede bloğun bütünlüğü bozulmuş olur. Her bir blok oluşturulduğunda bloğu oluşturan madenci diğer madencilere bu bloğu bildirir ve herkese yayınlar. Diğer madencilerde bu bloğu alıp kendi zincirlerine dahil ederler. Eğer aynı anda birden fazla blok yayınlanırsa ve zincirde bir çatallanma meydana gelirse madenciler bir süre sonra en uzun zinciri tespit edip onu ana zincir olarak kabul ederek çalışmaya devam ederler. Kabul edilmeyen zincirlerdeki bloklar yetim blok olarak adlandırılır.



Şekil 2.4. Blokzincirinde Merkle ağaç yapısı.

Yetim bloglar veri kaybına sebep olmazlar. Çünkü yetim bloklarda bulunan transactionlar diğer bloklarda da bulunurlar. Çünkü her madenci kendisine gelen transaction kendi belleğinde bloklara yerleştirmek amacıyla depolar. Buna transaction havuz bellegi denir ve bitcoin terminolojisinde mempool olarak adlandırılır. Madenciler kendilerine gelen her transactionı özellikle kendi belleklerinde depolarlar ve bu transactionlar bir blok içerisinde yerleştirildikten sonra ve o bloğun üzerinden bir miktar blok daha oluştuktan sonra o transactionın kalıcı olduğuna emin olurlar ve bellekten silebilirler. Bu sayede yetim bloklarda bulunan transactionlar bile kaybolmamış olur (Şekil 2.5).



Şekil 2.5. Blokzincirinde transaction pool ve blok ilişkisi

2.2.5. Blokzinciri Madenciliği

Blokzincir sadece bir veri yapısı olarak herhangi bir yenilik sunmaz. İşlemleri bloklar halinde tutmak ve blokları zincirler halinde birbirine bağlamak blokzincirle icat edilmiş bir şey değildir. Bir blokzinciri güvenli yapan şey bu blokların oluşturulma şeklidir. Blokzincir madencileri arasında bir rekabet ortamı oluştuğu zaman blokzincir güvenli olabilir. Yani her madenci bir sonraki bloğu oluşturabilmek için birbirleri ile yarışırlar. Bu yarışı her seferinde kimin kazanacağı belli değildir. Tamamen olasılıksal bir durumdur. Mesela bitcoin üzerindeki her bir madenci işlem gücünü kullanarak

birbirleri ile yarışır ve bir sonraki bloğu bulmaya çalışır. Bir madencinin işlem gücü diğer bir madencinin işlem gücünün iki katı ise o madencinin blok bulma ihtimali iki kat daha fazladır.

Madenciler arasında rekabet durumunun oluşması ortada teşvik edici bir sebebin bulunmasına bağlıdır. Mesela bitcoinde ve birçok diğer kripto paralarda bir bloğu bulmak size o bloğun ödülünü kazandırır. Yani her blok bir ödül içerir ve her madenci bu ödülü almak için yarışır. Bu rekabet ortamı sadece bir ödül ile oluşmak zorunda değildir. Mesela bir online seçim sisteminde madenciler bir ödül kazanmazlar ama ortak bir amaç için bir araya gelmişlerdir. Eğer madenciler farklı ve rakip partilerden ve çeşitli sivil toplum kuruluşlarından oluşursa bu rekabet ortamı sağlanmış olur.

Madenciler arasındaki rekabet bir blokzincirin var olabilmesi için en önemli şarttır. Bunun sağlamayan bir blokzincir, gerçek bir blokzincir değildir. Sadece bir veri tabanıdır ve %100 güvenli değildir. Çünkü rekabet ortamı oluşmazsa o zaman madencilerin ortak bir amaç uğruna bir araya gelip hile yapmadıkları garanti edilemez. Çünkü madenciler istemedikleri transactionları sansürleyebilirler veya protokol kurallarını değiştirmeye çalışabilirler.

Aslında klasik seçim sistemleri de bu prensiple işler. Seçim sisteminin güvenliğini gözetmenler sağlamaktadır. Gözetmenler farklı partilerden olduğu için doğal olarak gözetmenler arasında da rekabet bulunmaktadır. Bu sayede seçimin güvenliği sağlanmış olur. Bu durum blokzincir içinde geçerlidir.

2.2.6. Madencilik Algoritmaları

Blokzincir üzerinde madenciler arasındaki rekabeti sağlayan ve yeni blokların ortaya çıkışını belirleyen birçok algoritma bulunmaktadır. Bunların en önemlisi ve ilki, Bitcoin'in sahip olduğu **iş ispatı** (*proof-of-work*) algoritmasıdır. Bu algoritma madencilerin kendi aralarında işlem gücünü kullanarak yarışmasını sağlar. Bunun dışında **varlık ispatı** (*proof-of-stake*) algoritması da son zamanlarda oldukça yaygınlaşmıştır. Bunun dışında yarı açık blokzincirlerinin kullandıkları algoritmalar da vardır.

- **İş İspatı** (*Proof-of-work*)**:**

  Bitcoinin kullandığı bu algoritma işlem gücünü baz almaktadır. Bu algoritmanın temeli hash cache algoritmasıdır. Hash cache spam email gönderimini engellemek için düşünülmüştür. Email in özet bilgisi herhangi bir hash fonksiyonu ile hesaplanır ve ortaya çıkan sayının belli bir değerden küçük olması amaçlanır. Eğer sonuç istenilen değerden küçük değilse email in içerisine koyulmuş rastgele bir sayı değiştirilerek tekrar denenir. İstenilen değer bulunana kadar bu işlem tekrarlanır. Bu işlem milyarlarca kez tekrarlanabilir. Bu işlem her bilgisayar için belli bir zaman alacaktır. Ama sonuç olarak oluşan değerin istenilen maksimum değerden küçük olduğunu doğrulamak çok kolaydır. Bu sayede oluşturulması zor ama doğrulanması kolay bir sayı elde edilmiş olur. Böyle bir sayıyı içeren mailleri toplu olarak atılamayacağı ortadadır. Çünkü 100.000 mail atmak için dahi günlerce sürecek bir işlem yapmak gerekir. Ama tek bir mail atmak için bir iki saniye yeterlidir. Bu kabul edilebilir bir gecikmedir. Maili alan taraf aldığı mail içerisinde bulunan bu sayıyı kontrol eder. Bu sayı yapılmış bir işin ispatıdır. Bu nedenle buna iş ispatı (Proof of Work) denir.Bitcoin içinde benzeri bir yöntem kullanılır. Her madenci işlemleri bir blokta topladıktan sonra bu bloğun başlığını hash fonksiyonundan geçirir. Elde edilen özet sayısının belli bir değerden küçük olması amaçlanır. Elde edilen değer bu kriteri sağlayana kadar blok başlığındaki rastgele sayı alanı değiştirilerek tekrar denenir. Bu işlem ortalama 10 dakika sürer. Madencilerin işlem gücü arttıkça istenilen kriterde zorlaşır. Yani daha küçük bir değer elde etmek gerekir. Proof of work algoritması herkese açık olan blokzincirler için en iyi yöntemdir.

- **Varlık İspatı** (*Proof-of-stake*)**:**

  Bu algoritmada madenciler işlem gücünü kullanarak yarışmazlar. Ellerinde bulunan ve madencilik için ayırdıkları para miktarınca kazanırlar. Yani o blokzincire ait kripto paradan ayırıp ona göre yeni blokları bulma şanslarını belirlerler. Bu sistem aslında bir çeşit faiz sistemidir.

- **Sıralı Madencilik:**

  Herkese açık olmayan yarı kapalı bir blokzincir için daha sınırlayıcı bir

madencilik yöntemi kullanılması gerekir. Sıralı madencilikte madenci olabilecek kişiler önceden belirlenmiştir. Yani bir yetkilendirme söz konusudur. Madenci olacak kişiler önceden kendi gizli anahtarlarını (private key) oluştururlar ve açık anahtarlarını (public key) önceden bildirirler ve yetkisi olan madencilerin anahtarları yazılıma gömülür. Bu yöntemde madencilik herhangi bir işlem gücüyle veya bir kripto o parayla yapılmasına gerek yoktur. Her madencinin bir sonraki bloğu bulma ihtimali eşittir. Ayrıca genellikle bu tarz sistemlerde üst üste iki bloğun aynı madenci tarafından üretilmesi protokol kuralları gereği yasaktır. Bu yöntemde madenciler sahip oldukları gizli anahtarları korumaya özen göstermelidirler. Çünkü bu gizli anahtarlara ulaşılması madencilik yetkisinin de elde edilmesine sebep olur. Kısa süreli hayatta kalacak blokzincirler için tercih edilebilir bir sistemdir. Blokzincir tabanlı bir seçim sistemi için bu madencilik yöntemi oldukça uygundur. Çünkü böyle bir sistem hem yarı kapalı sistemdir. Hem de kısa süreli yaşayacak sistemdir. Bu sistemde rekabet ortamı sistemin kendi özellikleri arasında değildir. Ama madencilerin gerçek hayatta aralarında kendi rekabet halinde oldukları için bu sistemde de rekabet ortamı oluşmuş olur.

2.2.7. Online Seçim sistemi için blokzincir kullanımı

Blokzincir merkezi bir güven noktasını ortadan kaldırdığı için online seçim sistemleri için çok uygun bir mekanizmadır. Ama online seçim sistemi için kullanılacak blokzincir algoritması doğru seçilmelidir. Ayrıca bu tek başına yeterli değildir. Bir seçim sisteminin güvenliğinin başka unsurları da vardır.

Online seçim ve elektronik oylama sistemleri üzerine bugüne kadar birçok çalışma yapılmıştır. Ancak bu çalışmaların çoğunluğu blokzincirden daha öncesine dayanmaktadır. Bu nedenle önceki çalışmalar genelde merkezi bir yetkilendirme servisine bağlı olmaktadır veya sayım tam olarak halka açık bir şekilde yapılamamaktadır. Geçmişte yapılmış bu çalışmalar blokzincir ile birleştirilebilir.

Blokzincir kullanılarak seçim sistemi oluşturulması daha önce de başkaları tarafından ortaya atılmış bir fikirdir. Şu ana kadar oluşturulmuş blokzincir tabanlı seçim sistemlerinin her birisinin birbirlerine karşı avantajları ve dezavantajları söz konusudur.

Çünkü kullanılan blokzincir içerisinde oy kullanacak kişinin yetkilendirilmesi, bu sayede başka kimselerin oy kullanmasının engellenmesi gerekmektedir. Bunun aynı zamanda kişilerin kimliğini gizleyerek yapılması bazı zor durumları ortaya çıkarmaktadır.

Bazı ülkeler seçimler için blokzincir teknolojisini kullanmayı düşündüklerini açıkladıkları halde bu konuda nasıl bir çalışma yapıldığı çok açık değildir. Blokzincir tabanlı oylama ile ilgili öne çıkan bazı çalışmalar aşağıdaki şekildedir:

a) Rusya blokzincir teknolojisini seçim sonrasi sayım aşamasında oy pusulalarının taranıp gözetmenlerin huzurunda bir blokzincire yazılmasını ve bu şekilde daha şeffaf bir sayım yapılmasını sağlayan bir sistem üzerinde çalışmaktadır. Ama bu bir online seçim sistemi değildir (Castillo, 2018).

b) İngiltere Plymouth Üniversitesi'nde bir grup araştırmacı "Digital Voting with the use of Blockchain Technology" adında bir makale yayınlayarak, klasik seçim sistemi ile online seçim sistemini bir araya getirecek bir yöntem önermişlerdir (Barnes ve ark., 2017).

c) Polys Online Voting System: Bu sistem sıralı madencilik benzeri bir madencilik algoritması kullanan bir blokzincir kullanmaktadır. Ayrıca kullanılan oyların gizliliğini ve güvenliğini sağlamak için homomorphic encryption ve Secret sharing algoritmalarını kullanmaktadır. Bu sistemde kullanılan bütün oylar madencilerin belirledikleri anahtarlar ile homomorfik olarak şifrelenirler. Oylar şifrelenmiş olarak toplandıkları için kullanılan oyların doğru bir oy olup olmadığını anlamak için Zero-knowledge-proof algoritması kullanılmaktadır. Bu sistem güvenliği oldukça yüksek bir sistemdir. Bu sistemde Oyların sayımı oylama bittikten sonra yapılır bu diğer birçok sistemde var olmayan bir özelliktir ama çoğu seçim sisteminde var olması istenilecek bir özellik olduğu için bu sistem diğerlerinden ön plana çıkmaktadır. Oylama sırasında oylar şifrelidirler ve oylama bittikten sonra madenciler bir araya gelerek sadece sonucu çözümlerler, tek tek oyları çözümlemezler (Polys, 2017).

   Fakat bu sistem madencilerin oylama bittikten bir süre sonra bir araya gelip oyları tek tek çözmeye çalışmayacaklarını kabul etmektedir. Bu her zaman doğru

bir kabul olmayabilir. Bu nedenle bu Algoritma üzerine 2. seviye algoritmalar da eklenebilir.

d) FollowMyVote : Bitshares tabanlı bir çözümdür. Bitshares DPOS algoritması ile çalışmaktadır. FollowMyVote blinded-digital-signature algoritmasını kullanmaktadır (Followmyvote, 2017).

e) BitCongress adında bir blokzincir tabanlı seçim sistemi ise Bitcoin blokzinciri üzerinde ve Bitcoin üzerinde çalışan Counterparty protokolünü kullanarak çalışan bir sistemdir (Bitcongress, 2016).

3. MATERYAL VE YÖNTEM

Önceki bölümlerde blokzincir kullanılarak oyların toplanılması ve sayılması sürecinin nasıl yapılabileceğinden bahsedildi. Oyların gizliliği ve güvenliği konusunda blokzincir teknolojisi tek başına bir şey sunmaz. Fakat ilave bazı algoritmalar kullanılarak da eksik giderilebilir. Oyların yetkilendirilmesi şifrelenmesi ve hesaplanması aşamalarında kullanılabilecek birçok yöntem ortaya koyulmuştur. Bu konuda yapılan çalışmaların büyük bir çoğunluğu blokzincir resimden daha geçmiş tarihlere aittir.

3.1. Oyların Gizliliği Ve Güvenliği

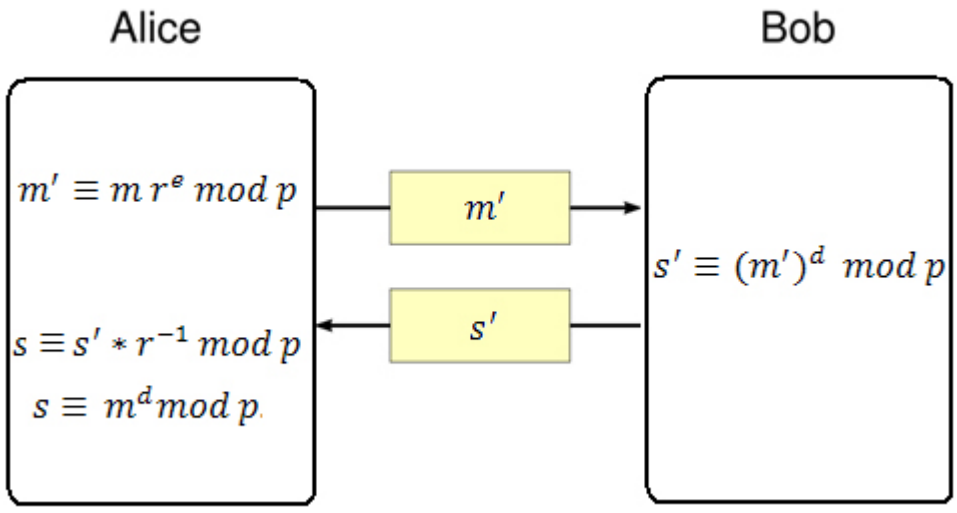
Bu bölümde blokzincir üzerinde oyların depolanırken hangi formatta tutulabileceği ve oyların madencilere gönderilirken nasıl gönderilebileceği konusunda kullanılabilecek kriptolojik protokoller anlatılacaktır.

Yarı kapalı bir blokchain de gerçekleştirilecek işlemlerin yetkilendirilmesi çok önemlidir. Ayrıca bunu işlemi yapan kişilerin gizliliğini koruyarak yapmak daha da zordur. Bu problemi çözmek için çeşitli yöntemler önerilmiştir. En yaygın kullanılan yöntemlerden birisi blind signature (gizli imzalama) kullanımıdır. Bu yöntem yardımcı bazı protokollere de ihtiyaç duyar. Bir diğer yöntem ise Secret sharing (gizli paylaşma) algoritması kullanılmasıdır. Ayrıca Ring Signature (halka imza) yöntemi de birçok seçim sistemi için önerilmiştir. Bu bölümde bu yöntemlerin avantajlarını ve dezavantajlarını inceleyeceğiz.

3.1.1. Kör imzalama

Kör imzalama (*blind signature*), David Chaum tarafından ortaya atılmış [12] bir kriptografik protokoldür. Yetkili bir tarafın gizli bir bilgiyi, o bilgiyi görmeden imzalamasını sağlamak için geliştirilmiştir. Bu yöntemde blokchain’den ayrı olarak bir yetkilendirme servisinin bulunması gerekir. Seçmenler oy kullanmadan önce rastgele bir gizli sayı oluşturup yetkilendirme servisine gönderirler. Yetkilendirme servisine giden bu anahtar değer bir örtülendirme (blinding) işleminden geçirilmiştir. Yetkilendirme servisi kendisine kimlik bilgileri verilen kişinin oy verme yetkisini ve daha önce gelip

gelmediğini denetleyerek oy kullanmaya hakkı olup olmadığına karar verir. Eğer oy kullanmaya hakkı varsa gönderilen anahtar değeri dijital olarak imzalar daha sonra geri gönderir. Oy kullanma sistemi bu imzalanmış anahtarın üzerinde örtülendirilmeyi kaldırma (unblinding) işlemi yapar. Bu sayede sadece kendisi tarafından bilinen gizli bir anahtarı, yetkilendirme servisine imzalatmış olur. Yetkilendirme servisi dahil kendisi dışında kimse bu değeri bilmemektedir. Bu anahtar değer oy pusulası olarak kullanılacaktır. Bu anahtar değer yetkilendirme servisi tarafından imzalandığı için madenciler tarafından kabul edilecektir. Aşağıda bu akış grafiksel olarak ifade edilmiştir (Şekil 3.1).



Şekil 3.1. Kör imzalama şeması

Burada Alice oluşturduğu gizli bir sayı olan r sayısı ile örtülendirme yapar ve geri dönen sayı için de aynı işlemin tersini yaparak çözümler. Yetkilendirme otoritesi Bob sonuç olarak m değerini görmeden imzalamış olur. Bu bir karbon kağıt kullanarak görmediğiniz belgeyi imzalamaya benzetilebilir.

Bu sistemde gönderilecek oylar gizli bir kanal üzerinden gönderilmelidir. Çünkü verilen oyun içeriği gizli olmadığı için gönderilen bilgisayarın IP ve benzeri bilgileri ile kimliği çözülebilir. Bu konuda alınabilecek ekstra tedbirler sonraki bölümlerde işlenecektir.

Bu sistemin en büyük problemi yetkilendirme servisinin kendi başına oy pusulası üretmesi ve imzalayabilmesidir. Aslında seçmen sayısını geçecek kadar oy pusulası üretemez ama oy kullanmayan kişi sayısının dikkat çekmeyecek bir miktarı kadar üretip seçimin bitmesine az bir süre kaldığında bu oyları sisteme dahil edebilir. Bu sorunu çözmek için bu sisteme ilave bir seviye daha eklemek gerekir. Ayrıca bir oy verildikten sonra tekrar değiştirilmek istenirse, bu sistemde onu yapmak mümkün değildir. Ama ek protokoller yardımıyla sağlanabilir.

3.1.2. Homomorphic Encryption

Homomorphic Encryption şifrelenmiş veriler üzerinde yapılan bir matematiksel işlemin çözüldüğünde sanki bu değerin şifrelemeden aynı matematiksel işlemden geçirilip sonra şifrelenmiş gibi sonuç verdiği bir şifreleme yöntemidir. Bu matematiksel işlem genelde toplama veya çarpma işlemidir. Mesela toplama işlemi üzerinde homomorphic olan bir H şifreleme algoritması olduğunu düşünelim. A ve B şifrelenmemiş asıl veriler olsun. Aşağıdaki eşitlik sağlanır:

$$H(A) + H(B) = H(A+B) \quad (1)$$

Benzeri bir algoritma çarpma işlemi içinde düşünülebilir. Yani H çarpma işlemine göre homomorphic bir şifreleme algoritması olsun. Aşağıdaki eşitlik sağlanır:

$$H(A) * H(B) = H(A*B) \quad (2)$$

Her tam sayı asal sayıların çarpımı şeklinde yazılabilir. Bunu bir seçim sistemindeki seçeneklerini birbirinden ayırmak için kullanabiliriz. Örneğin bir seçim sisteminde iki seçeneğin var olduğunu kabul edelim. Her bir seçenek için 2 ve 3 olmak üzere birer asal sayı seçilmiş olsun. Her bir oy 2 veya 3 sayısının şifrelenmiş hali olacaktır. Bu şifrelenmiş sayılar birbirleriyle çarpıldığında, bu sayıların çarpımının şifrelenmiş hali elde edilecektir. Bu sayede sonuç asal çarpanlarına ayrıldığında elde edilen asal çarpanların kuvvetleri kullanılan oy sayısını gösterir. İşlem adımları aşağıdaki gibidir:

- 1. *seçenek için seçilen çarpan* = 2
- 2. *seçenek için seçilen çarpan* = 3
- $S = 2^x \times 3^y$ | *S bu seçeneklerin çarpımından oluşan bir sonuçtur*
- x = 1. *seçenek için kullanılan oy sayısıdır*
- y = 2. *seçenek için kullanılan oy sayısıdır*

Burada her bir oy değil sadece sonuç değeri (S) çözümleme işleminden geçirilmelidir. Blokzincire kayıt edilmiş her bir oy şifrelenmiş haldedir ama sonucu çözmek için kullanılacak anahtar aslında her bir oyu da çözümleyebilir. Bu nedenle çözme işleminin sadece sonuç üzerinde kullanıldığına emin olmak için gizli paylaşım (Secret sharing) algoritmaları kullanılabilir. Bu yöntemde şifreleme için kullanılan anahtar aslında sonucu işleyecek tarafların sahip oldukları anahtarlardan elde edilmiştir. Ve şifreyi çözmek için anahtarların en az önceden belirlenen bir adedi bulunmalıdır. Bir blokzincir sisteminde bu anahtarlar madencilere ait anahtarlar olabilir. Mesela 100 tane madenci olduğunu kabul edelim 100 anahtardan bir anahtar değer üretilir ve bu şifreleme için kullanılır. Şifreyi çözmek için bu anahtarlardan en az 70 tanesinin gerektiğini düşünelim. Bu değer önceden belirlenmiştir. Madencilerin her bir oyu tek tek değil de sadece sonucu çözmek için bir araya geleceğini kabul edersek bu durumda oyların gizliliği sağlanmış olacaktır. Fakat bunu garanti etmek mümkün değildir. Yani madencilerin bir araya gelip oyları tek tek çözümlemeye çalışmaları mümkündür. Fakat çok düşük bir ihtimaldir. Burada eğer oyların her birinin kime ait olduğu da gizlenirse buna gerek kalmayacaktır. Ama bu aynı zamanda homomorphic encryption da gereksiz hale getirmektedir. Çünkü zaten her bir oy herhangi bir kişiyle ilişkilendirilmiyor ise oyların şifrelenmesine gerek yoktur. Ama seçim sonuçlarının sadece oylama bittikten sonra belli olması isteniyorsa yani oylama sırasında ara sonuçların belli olmaması isteniyorsa ikisi bir arada kullanabilir.

3.1.3. Gizli Paylaşım

Gizli paylaşım (*secret sharing*) algoritması belli bir grup katılımcı arasında gizli bir bilginin parçalara ayrılarak taraflar arasında dağıtıldığı bir sistemdir. Katılımcıların hiçbiri bu gizli bilginin tamamını erişemez. Bu gizli bilgiyi elde etmek için katılımcılardan bir kısmı bir araya gelmelidir. En meşhur gizli paylaşım algoritması Adi Shamir tarafından geliştirilmiş Shamir's Secret sharing algoritmasıdır.

Bu algoritma polinomun katsayılarını bulmak için gerekli minimum nokta sayısı prensibine dayanır. Mesela bir doğrunun denklemi en az iki nokta verilirse bulunabilir veya bir parabolün denklemi en az iki nokta verilirse bulunabilir. Doğal olarak k. dereceden bir polinomun katsayılarını ne bulmak için k+1 nokta verilmelidir.

Gizli paylaşma algoritmasında n katılımcı arasında bir bilgi paylaşılırsa ve n>k>1 olmak üzere en az k adet katılımcının bir araya gelmesiyle bu bilginin çözülmesi isteniyorsa k-1 dereceli bir polinom oluşturulup paylaşılmak istenen gizli bilgi bu polinomun sabit değeri olarak belirlenir ve o polinomun farklı x değerleri için n tane değeri hesaplanır ve n katılımcıya dağıtılır. Bu bilgi çözülmek istenildiğinde en az k tane değer alınıp polinomun katsayılar bulunur ve x=0 için polinomun değeri hesaplanır. Bulunan bu değer paylaşılan gizli bilgidir.

Bu seçim sisteminde kullanılan oylar madenciler tarafından hemen görülmemesi için ve oylama bittikten sonra madencilerin bir araya gelerek sonucu çözümlemesi için gizli paylaşım algoritması kullanılabilir. Bu sayede seçim sürecinde kullanılan oylar gizli olacaklardır. Seçim bittikten sonra madenciler sadece sonucu çözümlemek için bir araya gelecekleri için oylar gizli kalacaktır. Ama sonuç çözümlenmiş olacaktır. Bu yöntem homomorphic encryption kullanılarak uygulanabilir. Bu sayede her bir uyu çözümlemek gerekmez. Oyların şifrelenmiş halleri üzerinde matematiksel işlem yapılır ve sadece sonuç çözümlenir.

3.1.4. Zero-knowledge Proof

Bilgisayar bilimlerinin bir çalışma alanı olan veri güvenliği konusunda kullanılan bir algoritmadır. **Sıfır bilgi protokolü** (*zero knowledge protocol*) ismi de

verilir. Bir bilginin içeriği o bilgi açığa çıkarılmadan ispatlamaya yarar. Aslında “Bir bilgiyi bildiğimi, karşı tarafa bu bilgiyi vermeden nasıl ispat edebilirim?” sorusuna cevap arar. Bu algoritma online oylama sistemlerinde gerekli olabilir. Mesela homomorphic encryption kullanan algoritmalarda bu algoritma gereklidir. Çünkü gönderilen oyun sayısal değeri şifrelenmiş olduğu için o değerin sadece belli sayılar olduğu ve başka bir sayı olmadığı ispatlanmalıdır. Ama burada sayının kendisi ortaya çıkmamalıdır.

3.1.5. Halka İmza

Halka imza (*ring signature*) algoritması birden fazla kişinin açık anahtarını bir araya getirip tek bir anahtar üretip kullanmasıdır.

3.2. Oy Kullanması Sırasında IP Adresi Gizlenmesi

Oyların blokzincire gönderilmesi sırasında madenciler tarafından kişilerin IP adresleri ve buna benzer bazı bilgiler depolanabilir ve bunlar çeşitli amaçlarla analiz edilmek için kullanılabilir. Ayrıca blokzincir üzerinde oyların şifrelemenden tutulduğu bir algoritma seçilirse bu çok daha tehlikeli bir hal alacaktır. Böyle bir durumda madenciler her IP için kullanılan her oyu da göreceklerdir. Oyların şifreli olduğu durumda ise bu tehlike çok daha düşüktür. Ama böyle bir durumda dahi IP adreslerini gizlemek ekstra bir güvenlik oluşturacaktır.

Bizim burada önereceğimiz algoritma oyların onion routing benzeri bir karıştırma algoritması ile blokzincire gönderilmesidir. Onion routing bir paketin birden fazla alıcıya belli bir yolu izleyerek gönderilmesini ve gönderilirken geçtiği her bilgisayarda bir katmanının çözümlenmesini gerektirir. Yani her alıcı sadece kendine paketi gönderen ve bir sonraki alıcıyı bilecektir. Ama en son hedefi veya ilk gönderiyi bilmemektedir. Paket ilk oluşturup gönderilirken geçeceği her bilgisayar için bir şifreleme işleminden geçer. Önerdiğimiz seçim sisteminde bu aracı bilgisayarlar yine madencilerin kendisi olacaklardır.

Oy kullanma yazılımı bir oyu göndermeden önce belli bir sayıda madenciyi seçer ve bu madencilerden göndereceği paket için bir yol oluşturur. Paket geçeceği her

madencinin açık anahtarı ile şifrelenir. Aslında paket her seferinde bir zarfa konulmuş olur. Her zarfa konulduğunda o zarfı alacak madencinin açık anahtarı ile şifrelenmiş olur ve zarfın içerisine bir sonraki madencinin açık anahtarı yazılır. Yani her madenci kendisine gelen paketi kendi gizli anahtarı ile çözer ve paket içerisinden çıkan bilgi bir oy ise onu kendi oy havuzuna alır. Ama oy değil ise yani yeni bir paket ise paketin bir sonraki alıcısı olan madenciye gönderir.

Bu yöntemde gönderilen paketlerin hedefine ulaşmama ihtimali vardır. Çünkü her madenci her zaman ulaşılabilir olmayabilir. Bu durumun önüne geçmek için birden fazla rota oluşturulup hepsi aynı anda gönderilebilir. Bu durumda hedefine ilk ulaşan paket sayılacaktır diğerleri tekrar olduğu için göz ardı edilecektir.

3.3. Oy Kullanma Sürecinin Güvenliği

Bir online seçim sisteminde sistemin kendi güvenliği dışında oy kullanmak amaçlı kullanılacak cihazların güvenliği de çok önemlidir. Bunlar oy kullanma makineleri, web sitesi veya cep telefonu uygulamaları olabilir. Oy kullanılacak bilgisayarın veya telefonunun virüs içermesi veya bir oy kullanma makinesinin ele geçirilmiş ve değiştirilmiş olması durumunda oy kullanma sürecinin güvenliği tehlikeye girmiş olur.

3.3.1. Online Oy Kullanma Güvenliği

İnternet üzerinden oy kullanırken her bir seçmen kendine ait şahsi bilgisayarından veya akıllı telefondan oy kullanabilir. Bu durum kendi başına ciddi bir güvenlik problemi oluşturabilir. Seçim sistemini hedef alan saldırganlar bilgisayarlar ve telefon için virüs yazılımlar geliştirip oy kullanma sürecini bozabilir veya hile yapabilirler. Bir diğer tehlike ise taklit uygulamalar ve internet sitesidir. İnsanların yanıltarak telefonlarına yanlış bir uygulamayı yüklemeleri sağlanabilir veya yanlış bir internet sitesine yönlendirilebilirler. Ayrıca DNS yönlendirme saldırıları da kullanıcıların yanlış bir siteye yönlendirmek için kullanılabilir.

Bu tür saldırıların önüne geçmek için iki yöntem kullanılabilir. Bunlardan birincisi kullanılan bir oyun daha sonra doğrulanabilmesidir. Seçmenler oy kullandıktan sonra başka bir cihazda mesela cep telefonunda kullandıkları oyun doğru bir şekilde

kaydedilip kaydedilmediğini kontrol edebilirler. Bu sayede kullandıkları oydan emin olurlar. Ayrıca kişilerin kullandıkları oyu daha sonra oylama süresi bitmeden tekrar değiştirebilmeleri sağlanabilir. Eğer bu sağlanabilirse baskı altında oy kullanma tehlikesi de azaltılmış olacaktır. Çünkü insanlar baskı altında oy kullansa dahi daha sonra oylarını değiştirebilirler. Ayrıca web sitesinin ve telefon uygulamasının güvenliğini sağlamak için ekstra önlemler alınabilir.

Oy kullanmak için kullanılacak web sitesi tamamen istemci tarafında çalışacak şekilde JavaScript ile geliştirilmelidir. Bu kod seçim öncesi herkesin inceleyebileceği şekilde açık kod olacak şekilde paylaşılmalıdır. Bu herkese açık sistemler üzerinden yapılmalıdır. Herkes kaynak kodu görebilmeli ve inceleyebilmelidir. Ayrıca web sitesinin kullanıldığı gün yani seçim günü sitenin önceden yayınlanmış kod ile çalıştığını bağımsız uzmanlar sürekli olarak incelemelidir ve hatta bunun nasıl yapılabileceğini halka açık olarak anlatmalıdırlar. Bu sayede seçimin güvenliğini doğrulamak isteyen herhangi bir vatandaş da bunu yapabilir olacaktır. Aynı şekilde yayınlanan akıllı telefon uygulamaları da sadece doğru kanallardan yüklenecek şekilde halk eğitilmeli ve daha önceden yayınlanmış dijital imzalar kullanılarak doğrulama yapılmalı ve diğer insanların da bunu yapabilmeleri sağlanmalıdır.

4. ARAŞTIRMA VE BULGULAR

Blokzincir tamamen açık bir sistem olduğu için herkes bu sisteme katılabilir. Bu nedenle oy kullanımın yetkilendirilmesi ve gizliliğinin sağlanması ekstra önlemler alınmasını gerektirmektedir. Burada hem seçmenin yetkilendirilmesi hem de blokzincir madenciliğinin yani oyların toplanması ve işlenmesinin yetkilendirilmesi de önemlidir.

4.1. Önerilen Madencilik Sistemi

Bir seçim sistemi aslında halka açık bir sistem olsa da yarı kapalı sistemdir. Bu nedenle açık blokzincir algoritmaları kullanılması yeterli olmayacaktır. Bitcoin'in kullandığı Proof of work algoritması madencilerin hesaplama gücüne bağlı olarak blok üretebilmelerini sağlar. Tabii ki bu sistem olasılıksal bir sistemdir. Bitcoin de madencilerin yetkilendirilmesi bulunmamaktadır. Bu nedenle herkes madenci olabilir. Ayrıca bazı kripto paralar tarafından kullanılan Proof of stake algoritması da bu tarz biz karakteristiğe sahiptir. Bu algoritmalar yarı kapalı bir sisteme uygun değildir.

Önerilen madencilik yöntemi sıralı ve yetkilendirilmiş madenciliktir. Bu sistemde madencilik yapabilecek taraflar önceden belirlenmiştir. Bu taraflara ait **açık anahtarlar** (*public key*) önceden belirlenecektir. Madenciler kendi private key lerini kullanarak blogları imzalayacaktır. Art arda 2 blok aynı madenci tarafından imzalanamayacaktır. Bunun dışında imzalamalar rastgele olarak yapılacaktır. Bu sistemdeki madencilerin birbirleri arasında rekabet halinde olmaları çok önemlidir. Bu sayede güvenlik sağlanabilir. Madencilerin en fazla yarısı anlaşabilmelidir. Eğer madencilerin yarısından fazlası anlaşarak hile yapmaya çalışırsa gelen oyların bazılarını bloklara girmesine engelleyebilirler. Yani sansür yapabilirler. Mesela rekabet ortamı muhalefet partilerinin de madencilik yapması sağlanarak oluşturulabilir. Hatta partiler ve gönüllü sivil toplum kuruluşları bu sistemde madencilik yapmalıdırlar. Bu sayede madenciler arasında bir rekabet ortamı oluşturulmuş olacaktır.

4.2. Blokzinciri Üzerinde Oy Gizliliği ve Yetkilendirme

Önceki bölümlerde bahsedilen algoritmaların büyük bir kısmı büyük ölçüde oy güvenliğini sağlamaktadır. Ama bahsedilen algoritmalar arasında birçok avantaj ve

dezavantaj söz konusudur. Bu çalışmada önerilen sistemde secret sharing algoritması ve blind signature algoritmasından yararlanılacaktır.

Bu sistemde kullanılan oylar yetkilendirme servisi tarafından dijital olarak imzalanacaktır. Ayrıca kullanılan oyun bir halka imza yardımı ile hangi bölgeye ait olduğu bilinecek ve bu sayede bölge bölge ayrı sonuçlar da hesaplanabilecektir. Oyların seçim sürecinde yani oylama bitmeden önce sonuçlarının bilinmemesi için secret sharing algoritmasından yararlanılacaktır. Yani oylama bittikten sonra madenciler bir araya gelecek ve oyların çözümleme işlemi yapılacaktır.

5. ÖRNEK UYGULAMA

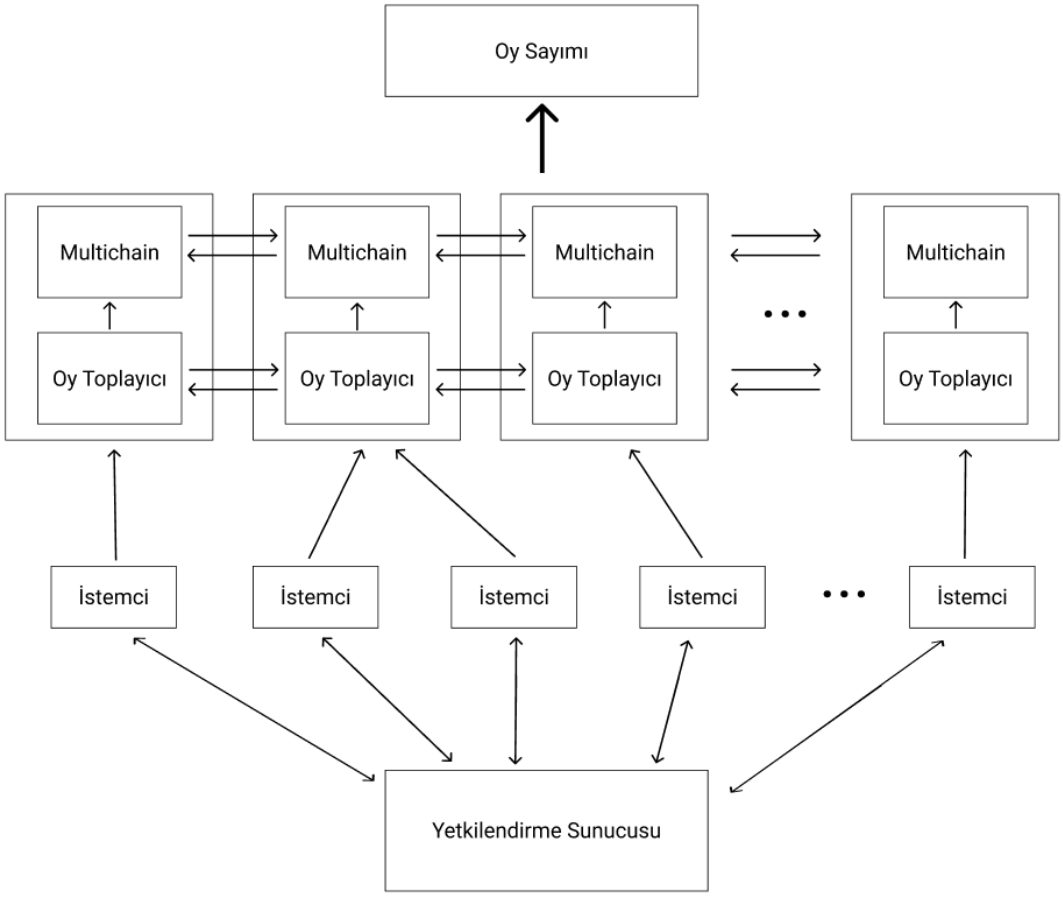
Bu çalışmada blokzincir tabanlı bir öneri oylama sisteminin geliştirilmesinin nasıl olacağını anlamak için örnek bir yazılım geliştirilmesi yapılmıştır. Bu yazılım bütün gerekli güvenlik özelliklerine sahip olmasa dahi, böyle bir sistemin kabaca nasıl yapılabileceğini gösteren bir prototiptir. Bu sistemde temel blokzincir görevini üstlenmesi amacıyla hazır bir blokzincir yazılımı olan Multichain kullanılmıştır.

5.1. Sistemin Genel Yapısı

Sistem genel olarak blokzincirin parçası olan sunuculardan ve bunlara yardımcı diğer yazılım parçalarından oluşmaktadır. Blokzincir düğümleri önceden belirlenmiş kişi veya kurumlar tarafından yönetilmektedir. Sistemde blokzincir sunucuları ve onlarla birebir bağlı oy toplayıcı programlar bulunmaktadır. Bunlar bir arada oyların toplanması geçerliliğinin kontrolü ve blokzincir üzerine kalıcı olarak yazılmasından sorumludurlar. Ayrıca sistemde oy kullanacak kişilerin yetkilendirilmesini yöneten bir yetkilendirme sunucusu bulunmaktadır. Ayrıca seçmenlerin oy kullanabilmeleri için de bir istemci yazılımı gereklidir. Bu yazılım bir web sayfası veya masaüstü ve mobil uygulama olarak da bulunabilir.

İstemci yazılımı önce yetkilendirme sunucusuna bağlanarak oy kullanabileceğini ispatlayacak ve aldığı yetkiyle oyunu kullanabilecektir. Yani önce yetkilendirme sunucusundan yetki alacak daha sonra oy toplayıcılara gizli bir şekilde oyunu ulaştıracaktır.

Son olarak oylama tamamlandığında oyların sayılabilmesi için oy sayım yazılımı kullanılacaktır. Bu program blokzincire bağlanacak ve birden fazla blokzincir sunucusundan blok zincirini alacak ve en uzun blok zincirindeki bütün geçerli oyları sayıp sonucu hesaplayacaktır. Sistemin genel yapısı aşağıda şema olarak gösterilmiştir. (Şekil 5.1.)



Şekil 5.1. Sistemin genel yapısı

5.2. Multichain

Prototip yazılımda temel blokzincir işlevlerini yerine getirmesi amacıyla Multichain adında hazır bir yazılım kullanılmıştır. Bu işlevler private (kapalı veya yarı kapalı) blokzincir için gerekli sunucu ve ağ altyapısını sunmak, yetkilendirme mekanizmasını sağlamak ve her türlü veri yapısının saklanabileceği bir blokzincir veritabanını sunmaktır.

Multichine Stream adında veri depolama amaçlı kullanılan blokzincir tabanlı bir mekanizma sunmaktadır. Stream üzerine veri yazabilme yetkisi herkese açık veya belli adreslere özel hale getirilebilir. Multichainin bu kısıtlama özelliği bu projede kullanılmayacaktır. Çünkü multichainin önüne, gelen oyları toplayan ve yetkilendirmesini doğrulayan bir katman konulacaktır. Bu sayede blokzincir sadece

yetkilendirilmiş oylar eklenebilecektir. Yani Multichainin sahip olduğu yetkilendirme mekanizmaları kullanılmayacaktır. Genel bir veri depolama arayüzü olarak kullanılacaktır.

Bu sistemde yeni blokların üretilmesinde kullanılan madencilik algoritması, sadece önceden belirlenmiş madenciler arasında rastgele olarak yeni bloklar üretilmesini sağlayan sıralı madencilik yöntemidir. Bu sistemde sadece önceden belirlenmiş adreslerin ürettiği bloklar kabul edilir. Bunlar izin verilmiş madenciler listesinde tutulur. Bu sayede sisteme yabancı bir madencinin girmesi engellenmiş olur.

Bu madencilik algoritmasında aynı madenci tarafından belli bir aralıkta üretilebilecek blok sayısını sınırlayarak blok üretimini madenciler arasında dağılmasını sağlayacaktır. Mesela her 10 blok aralığında aynı madenciden maksimum 2 blok oluşabileceğini ele alırsak blokların üretimi madenciler arasında dağılmak zorunda kalacaktır ve bu kurala uymayan zincir diğer madenciler tarafından kabul edilmeyecektir. Multichain ile bir blokzincir oluşturulduğu zaman verilen parametreler içerisinde **madenci çeşitliliği** (*mining diversity*) adında bir parametre ile bu durum ayarlanabilir. Bu algoritma round-robin algoritmasına benzemektedir.

5.3. Yetkilendirme Sunucusu

Oy kullanacak bir seçmenin oy kullanma hakkının olup olmadığını ve daha önce oy kullanmış olduğunu kontrol etmek amacıyla yetkilendirme sunucusu kullanılır. Oy kullanmak için kullanılacak istemci yazılım önce yetkilendirme sunucusu ile irtibata geçer ve çeşitli yöntemlerle kimliğini ispat eder. Daha sonra kendi oluşturduğu oy anahtarını bir gizleme işleminden geçirdikten sonra yetkilendirme sunucusuna gönderir. Burada kullanılan algoritma Blinded signature algoritmasıdır. Blinded signature yani kör imzalama algoritmasıdır. İstemci oy anahtarını blending denilen bir gizleme işleminden geçirir. Bu sayede yetkilendirme sunucusu oy anahtarını imzalarken imzanın gerçek değerini görmez. İstemci imzalanmış değeri aldıktan sonra unblinding denilen bir çözümleme işleminden geçirir. Sonuç olarak oy anahtarının yetkilendirme sunucusu tarafından imzalanmış hali elde edilmiş olur.

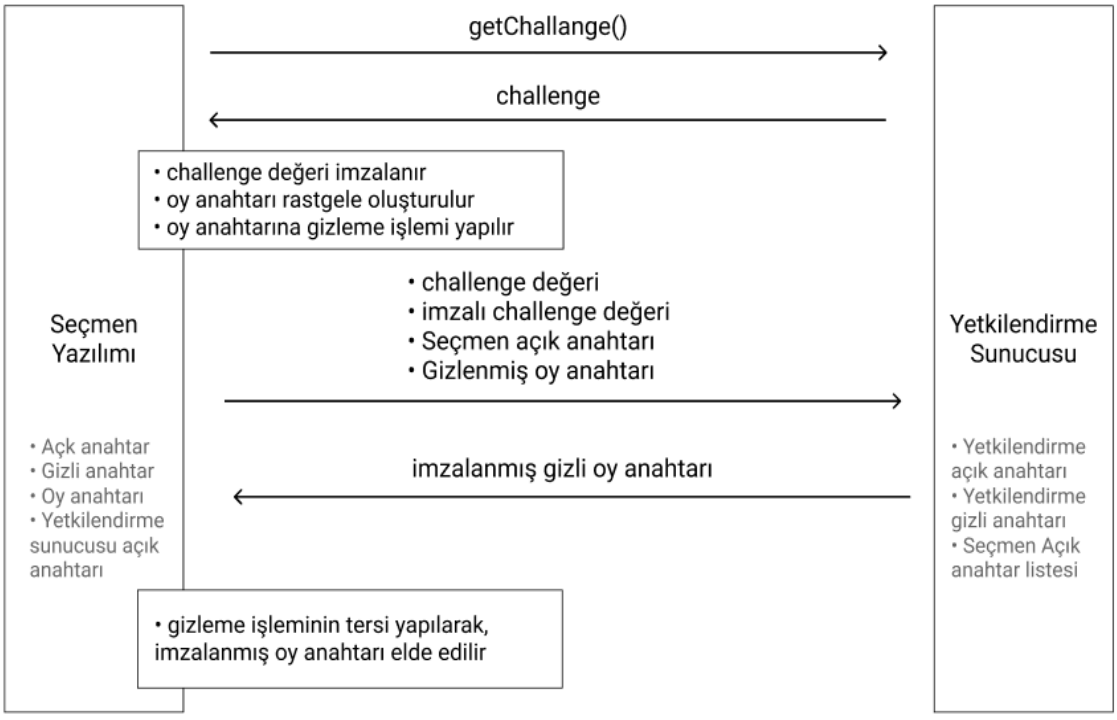
Yetkilendirme sunucusunun seçmenin kimliğini doğrulamak için iki farklı yöntem kullanılabilir. Birinci yöntem bir açık anahtar altyapısı kullanmaktır.

Mesela yeni nesil kimlik kartları buna güzel bir örnektir. İkinci yöntem ise güvenilir bir web sitesini yetkilendirme amaçlı kullanmaktır. Bir kullanıcı adı ve şifre ile giriş yapılabilen bir e-devlet uygulaması buna örnektir.

5.3.1. Açık Anahtar Altyapısı

Yetkilendirme aşamasında yeni nesil kimlik kartları gibi bir açık anahtar altyapısı kullanmak oldukça güvenlidir. Burada seçmenin sahip olduğu gizli anahtar sadece seçmenin elinde olduğu için ve başka hiçbir kurumun elinde olmadığı için bunu kullanarak oy kullanacak kişilerin kimliği doğrulanabilir. Böyle bir sistemde ya kişi gizli anahtarı elinde bulundurur veya bir kart okuyucu yardımıyla kullanılır.

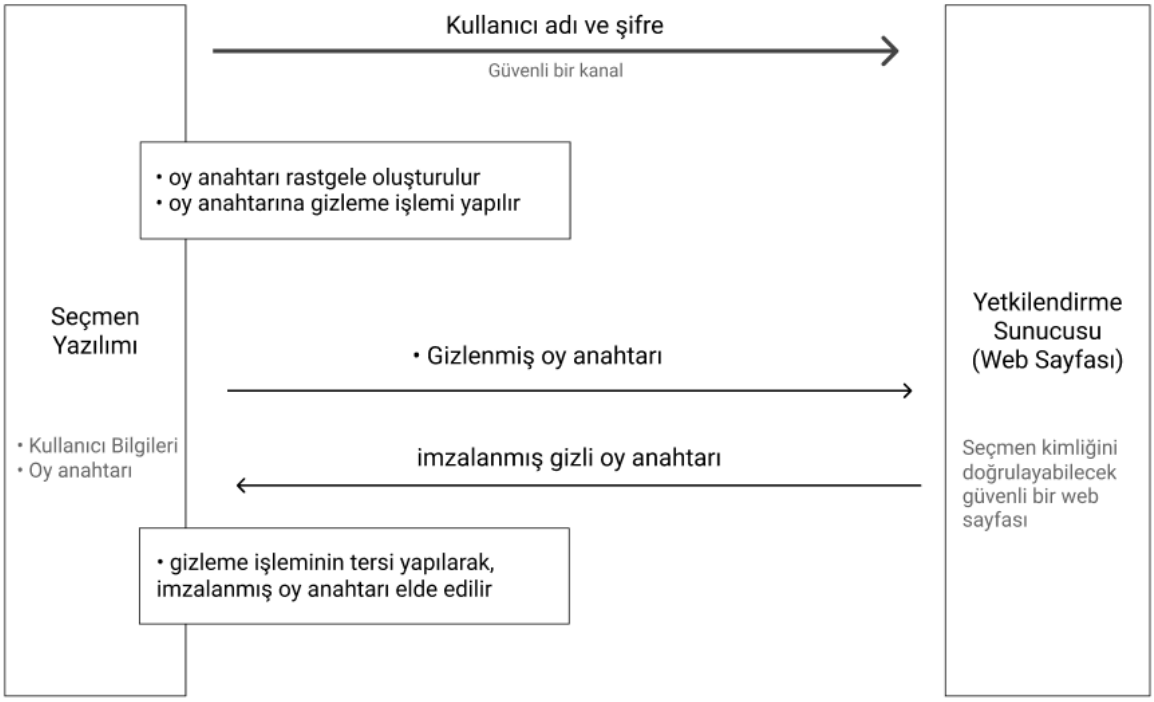
Bu yöntem ve yetkilendirme sunucusu rastgele bir Challenge (meydan okuma) değeri üreterek istemciden bunu imzalamasını ister. Eğer istemci bu değeri doğru bir şekilde imzalayabilir ise seçmenin kimliği doğrulanmış olur. Bu durumda istemci tarafından gönderilen gizleme işleminden geçirilmiş oy anahtarı kör imzalama yöntemi ile imzalanır. Böylece yetkilendirme işlemi tamamlanmış olur. Bu akış Şekil 5.2’de gösterilmiştir.



Şekil 5.2. Açık Anahtar altyapısı ile yetkilendirme

5.3.2. Güvenilir Bir Web Sayfası Kullanımı

İkinci yetkilendirme yöntemi ise sistem tarafından güvenli bir web sayfasına kullanıcı adı, şifre ve tavsiye edildiği üzere iki adımda doğrulama kullanılarak giriş yapılabilen bir sistem kullanmaktır. E-devlet sistemleri buna örnek verilebilir. Bu yöntemde kullanıcı giriş yaptıktan sonra seçmenin kimlik doğrulama işlemi tamamlanmıştır. İstemci önceki yöntemde olduğu gibi oy anahtarı oluşturup yetkilendirme sunucusuna kör imzalama yöntemi kullanarak imzalatır. Daha sonra bu anahtarı oy kullanmak için kullanacaktır. Bu yöntemin aşamaları aşağıda gösterilmiştir (Şekil 5.3.).



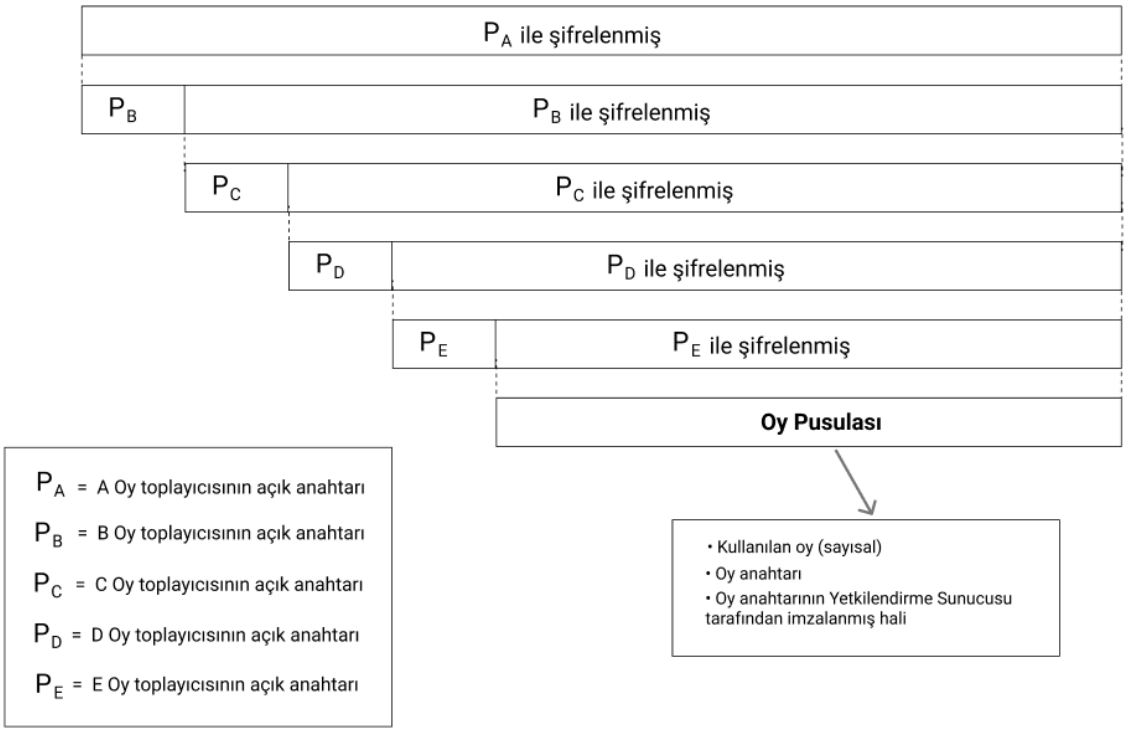
Şekil 5.3. Güvenilir Bir Web Sayfası ile Yetkilendirme

5.4. İstemci Yazılımı

Seçmenlerin oy kullanmak amacıyla kullanacakları yazılımdır ve birçok çeşidi olabilir. Bir web sayfası olabileceği gibi bir masaüstü veya mobil uygulama olabilir. Bizim bu çalışmada kullanacağımız örnek bir web sayfası olacaktır. İstemci yazılım en başından itibaren yetkilendirme sunucusunun ve bütün oy toplayıcıların açık anahtarını içermektedir. Bunlar istemci yazılıma gömülü olacaktır.

İstemci yazılım daha önceki bölümlerde anlatıldığı gibi öncelikle yetkilendirme sunucusuna bağlanarak oluşturmuş olduğu oy anahtarını imzalatır. Daha sonra bu oy anahtarını kullanarak oy pusulasını oluşturur. Daha sonra oy pusulasını gönderirken IP adresi gibi seçmenin kimliğini ortaya çıkarabilecek şeylerin gizli kalması için oy pusulasını tekrarlı olarak şifreleme işleminden geçirir. Yani oy pusulasını katmanlı olarak paketlemiş olur. Bu yöntem TOR ağında kullanılan “onion routing” yöntemine benzetilebilir.

Örnek bir oy pusulası aşağıda gösterilmiştir. (Şekil 5.4.)



Şekil 5.4. Bir oy paketinin katmanlı yapısı

Görüldüğü gibi oy pusulası katmanlı olarak şifreleme işleminden geçirilmiştir. Bir oy pusulası, oy toplayıcılar arasında aktarılarak her bir aktarım da bir seviye şifrelemesi çözülmüş olur. Her oy toplayıcı sadece kendinden önceki ve sonraki toplayıcıları bilmektedir daha ilerisini veya gerisini bilemez. Oy toplayıcılar kendi arasında anlaşmış olsalar dahi zincir içerisinde bulunan bir oy toplayıcının kurallara uyması ve bir hileye başvurmaması seçmenin kimliğinin gizli kalması için yeterlidir. Yani oy toplayıcıların belli oranda dürüst olması ve aralarında rekabet olması sistemin güvenliği için çok önemlidir.

İstemci yazılımın değiştirilmemiş olması çok önemlidir. Bu nedenle bu istemci yazılımın ve bu sistemdeki diğer bütün yazılımların kaynak kodları açık olmalıdır. İstemci yazılımın değiştirilip değiştirilmediği kontrol edilebilir olmalıdır. Mesela biz burada istemci olarak kullanılacak oy kullanma web sayfasının değiştirilmediğinin kontrolünün yapılabilmesi için bir yöntem öneriyoruz. Bu yöntem şudur. Web sayfası tamamen JavaScript programlama dili kullanılarak ve tek bir dosyadan oluşacak şekilde yazılmalıdır ve web sayfasının bu dosyadan başka bir kaynak kodu da olmamalıdır. Web

sayfasının HTML kodu sadece bu JavaScript dosyasını çağıracak şekilde olmalıdır. Ayrıca HTML dosyası JavaScript dosyasının Hash değerini de içermelidir. Bu sayede oylamanın güvenliğine yardımcı olmak isteyen kullanıcılar bu Hash değerini kontrol ederek kodlarda değişiklik olup olmadığını tespit edebilirler. Kullanıcıların çok küçük bir kesimi dahi bunu yaparsa sistemin güvenliğine çok büyük bir katkı sağlamış olur.

5.5. Oy Toplayıcı

Daha önceki bölümde multichainin gelen Transaction'lara herhangi bir filtre uygulamadığına değinilmişti. Bu filtrelemeyi sağlamak ve blokzincirinin geçersiz verilerle şişirilmesini engellemek amacıyla multichainin üstünde bir katman olarak, gelen verileri filtreleyen ve doğrulayan bir oy toplama yazılımı olacaktır. Bu yazılım gelen oyları inceleyecek ve geçerli olan oyları Multichaine iletecektir.

zOy toplayıcının iki temel görevi bulunmaktadır. Gelen oyları filtrelemek ve oy paketlerinin yönlendirilmesi.

5.5.1. Oyları Filtrelenmesi

Oy toplayıcı gelen oyları inceleyerek geçerli olanları blokzincire yönlendirir. Bir oyun geçerliliği içinde bulunan dijital imza ile kontrol edilerek yapılır. Bir oy pusulası üç kısımdan oluşmaktadır:

1. **Kullanılan oyun sayısal değeri:** Seçmen tarafından seçilen seçeneğin kodu
2. **Oy anahtarı:** Seçmen tarafından üretilmiş çok büyük bir rastgele sayı
3. **Oy anahtarının imzası:** Bu değer oy anahtarının yetkilendirme sunucusu tarafından oluşturulmuş imzasıdır. Bu gizli imzalama yöntemi ile imzalanmış bir değerdir. Bu imzanın geçerli olması oyunda geçerli olması anlamına gelir.

Oy toplayıcı program filtreleme yaparken oy anahtarını ve onun dijital imzasını kontrol eder ve geçerli olanları blokzincire yönlendirir.

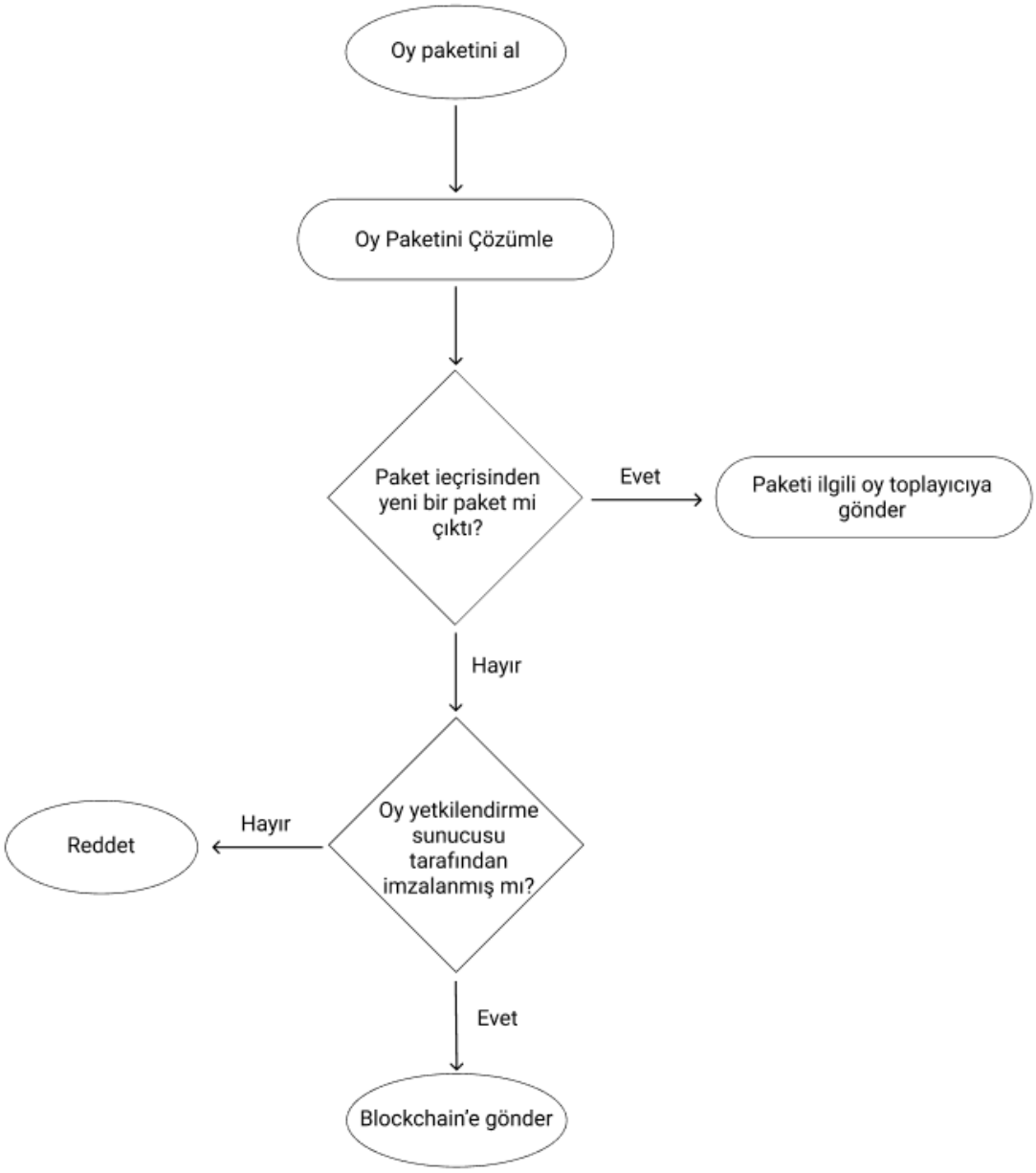
5.5.2. Oy Paketlerinin Yönlendirilmesi

Bir oylama sisteminde seçmenin kimliğinin gizliliği çok önemli olduğu için istemci yazılımda oy toplayıcıya oyları gönderirken gizli bir yöntem kullanılarak oyların gönderilmesi sağlanmalıdır. Bu sebeple seçmenlerin IP adreslerinin gizliliği çok önemlidir. Eğer oy toplayıcılar IP adresleri ile o adreslerden gelen oyları fişlemek ve analiz etmek amacı ile kayıt altında tutarlarsa birçok seçmenin oyunu tespit edebilirler.

Bu sistemde bunu önlemek amacıyla oylar şifrelenecektir. Şifrelenmiş oylar sadece seçilen belli oy toplayıcıların çözebileceği bir şekilde ve katmanlı olarak şifrelenecektir. Bu sayede bu şifrelenmiş oylar oy toplayıcılar arasında dolaşacaktır ve her bir adımda bir katman daha çözülmüş olacaktır. En son oy toplayıcıya gelindiğinde oy tamamen çözülmüş olacaktır.

Mesela bir oy 5 tane oy toplayıcı arasında dolaştırmak isteniyorsa 5 tane oy toplayıcının açık anahtarı rastgele seçilecektir. Daha sonra oy pusulası bu açık anahtarlar kullanılarak üst üste şifrelenecektir. Her şifreleme sırasında şifreleme içinde kullanılan açık anahtar şifrelenmiş verinin yanına eklenerek bir sonraki adıma geçilecektir. Böylece oy pusulası 5 defa paketlenmiş olacaktır ve her bir katmandaki paketi yalnızca bir oy toplayıcı çözebilir.

Sonuç olarak oy toplayıcılar kendilerine gelen bir paketi kendi gizli anahtarı ile çözüm dedikten sonra içinden çıkan veriyi kontrol ederler. Eğer oy pusulası ise geçerliliğini kontrol edip geçerliyse blokzincire yönlendirirler. Eğer paket içerisinden yeni bir paket çıkmışsa o paketi ilgili olan oy toplayıcıya gönderirler. Paketin gönderileceği oy toplayıcı paketin yanında bulunan açık anahtardan çözümlenecektir Bir oy toplayıcının genel çalışma mantığı aşağıda gösterilmiştir (Şekil 5.5.)

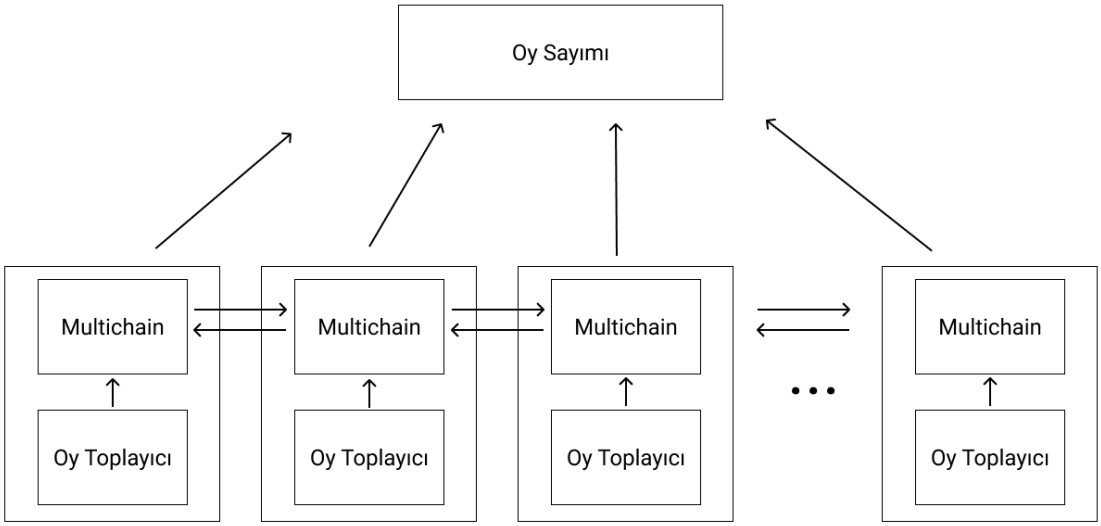


Şekil 5.5. Bir oy toplayıcının temel algoritması

5.6. Oy Sayımı

Oylama süresi dolduktan sonra oyların sayılma işlemine sıra gelmektedir. Oylar blokzincir üzerinde tutulduğu için oy sayımını yapacak olan yazılım blokzincire bağlanır ve blok zincirinin tamamını alır. Alınan veriler farklı blokzincir sunucularına bağlanarak alınmalıdır. Bu daha güvenlidir. Blokzincir alındıktan sonra bütün bloklar ve imzaları kontrol edilmeli ve sayılmalıdır. Ayrıca blokzincire herkes erişebilmeli ve bu sayımı yapabilmelidir. Ayrıca blokzincir üzerinde kendi oyunun bulunup bulunmadığı

da kontrol edebilir. Bu sayede hile yapılmış ise ortaya çıkmış olur. Bu şekilde oy sayımı yetkili kurumlar ile değil herkes tarafından yapılabilir olacaktır. Bu sayede seçmenin seçime daha fazla güvenmesini sağlayabilir.

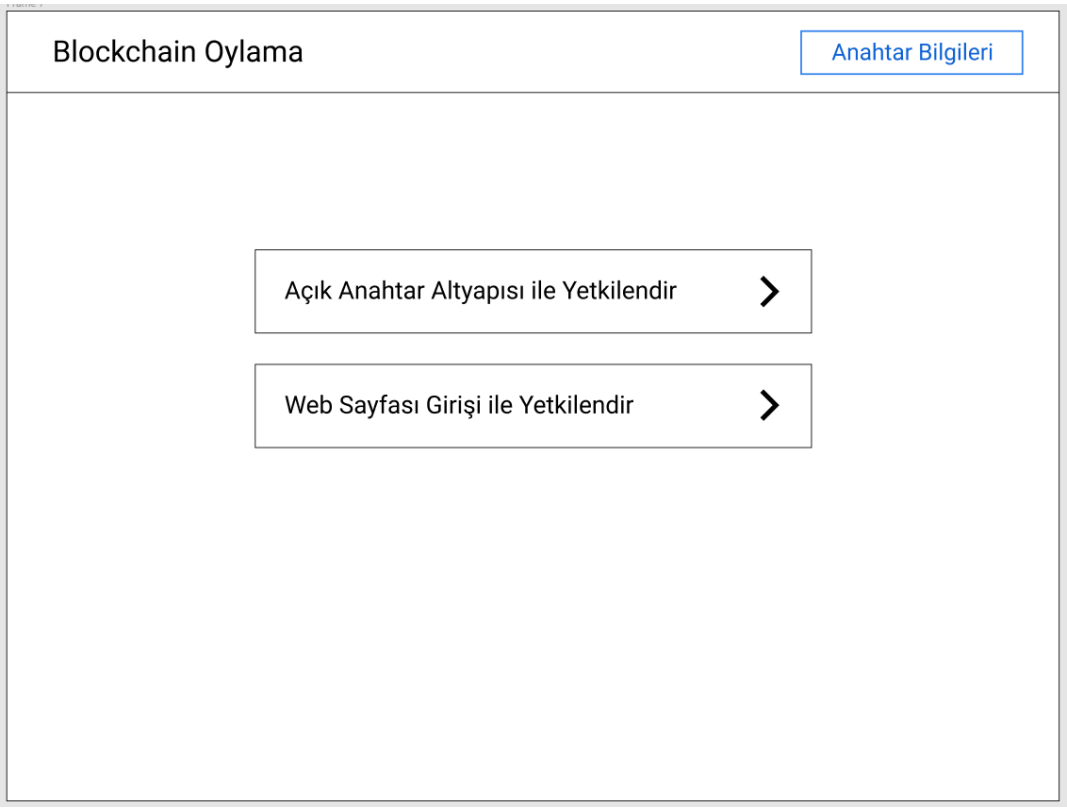


Şekil 5.6. Oy sayım süreci

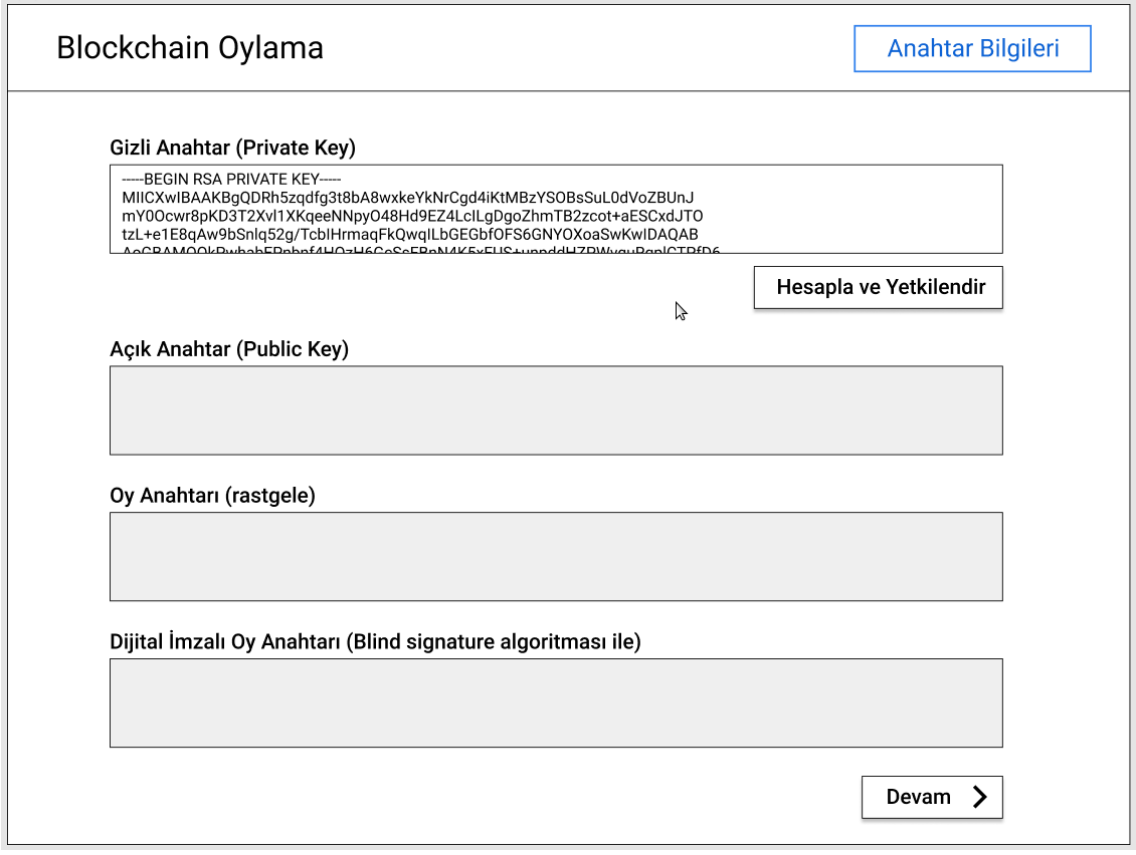
5.7. Uygulamanın Kullanımı

Bu uygulamanın genel olara görsel arayüzü, istemci yazılım yani oy kullanma yazılımı ve oy sayım aracından meydana gelmektedir. Diğer kısımlar büyük ölçüde görsel arayüzü olmayan yazılımlardır. Ayrıca Multichain içerisindeki kayıtları incelemek için Multichain Explorer yazılımı kullanılabilir.

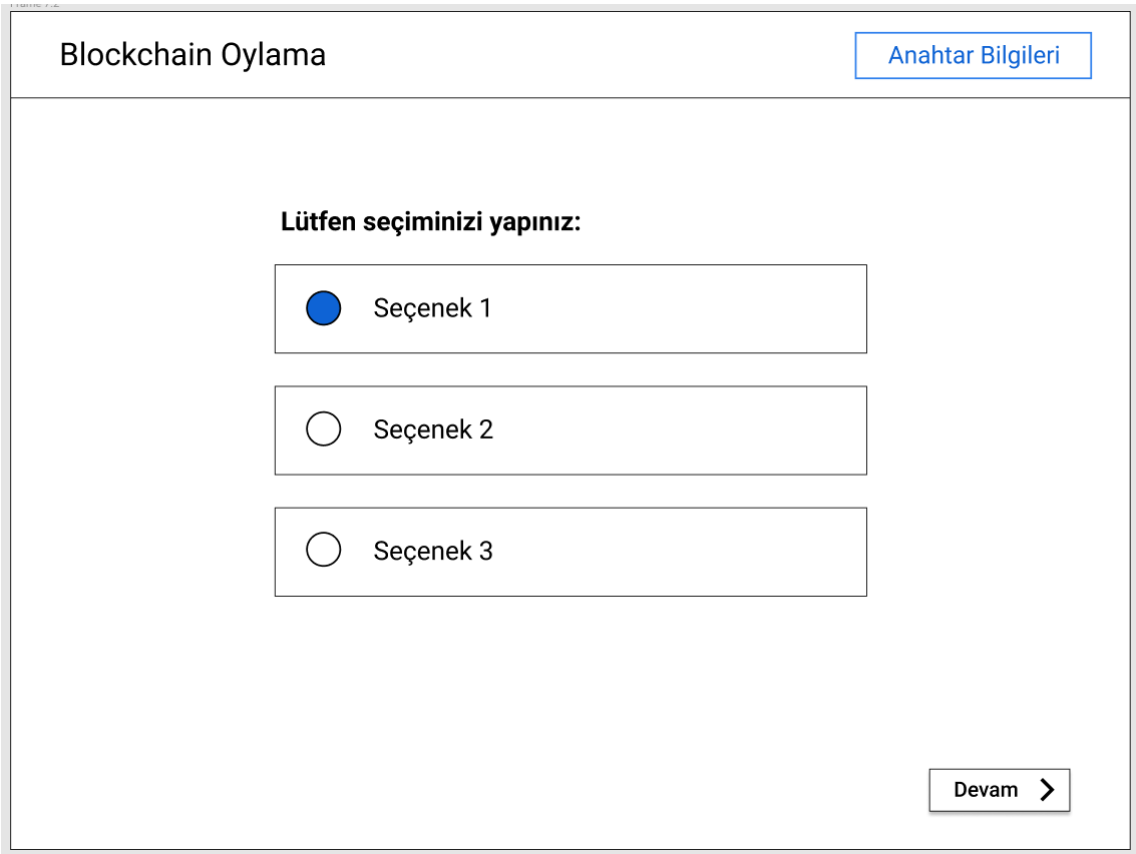
Oy kullanımı için istemci yazılım kullanılır. Burada kullanılan yazılım örnek bir web sayfasıdır. Bu nedenle bütün şifreleme ve dijital imzalama işlemleri javascript programlama dili kullanılarak geliştirilmiştir.



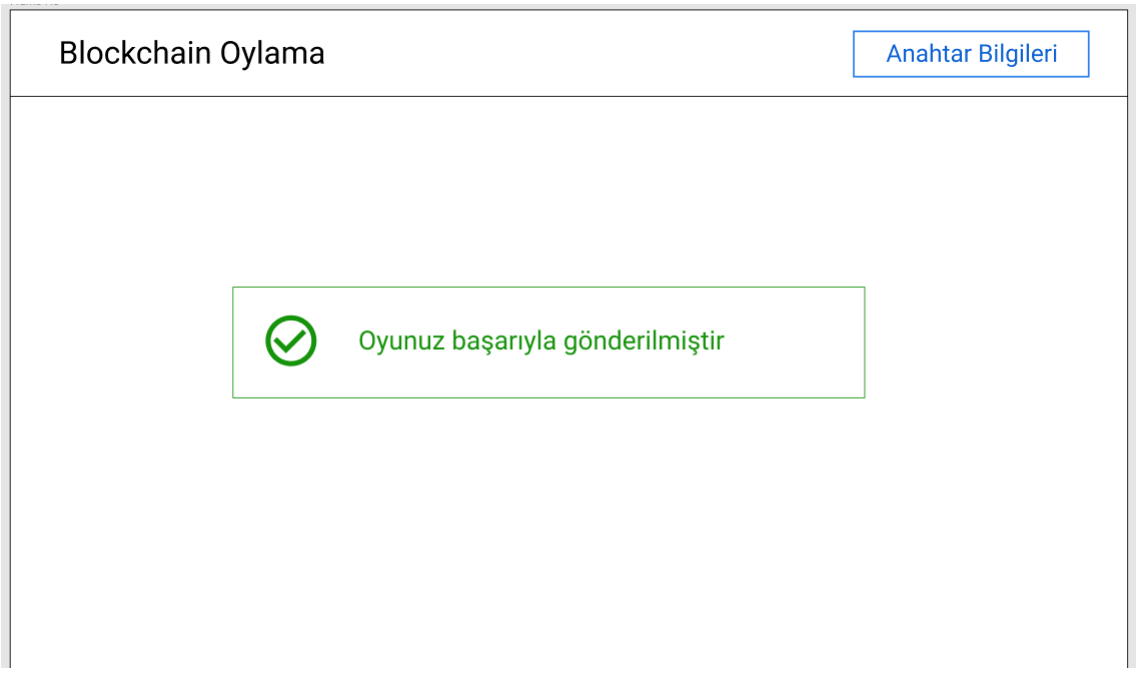
Şekil 5.7. İstemci birinci ekran



Şekil 5.8. Açık anahtar altyapısı kullanılarak yetkilendirme

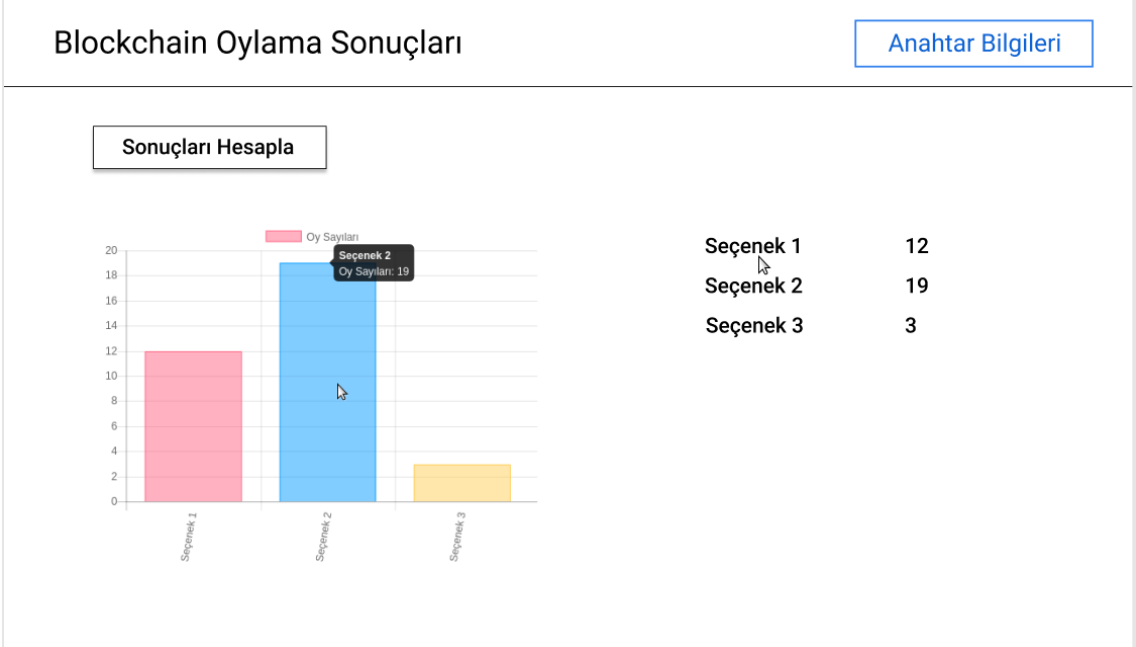


Şekil 5.9. Oylama aşaması



Şekil 5.9. Sonuç aşaması

Oy kullanma süreci tamamlandıktan sonra oy sayım sayfası oylamanın sonucunu görmek için kullanılır. Bu sayfa oy toplayıcıları kullanarak Multichain'e bağlanacak ve blockchainden oyları çekerek sayım yapacaktır.



Şekil 5.10. Oy sayımı ekranı

Bu uygulamanın bütün oyları blokzincirinden indirmesi biraz zaman alabilir ama bu sistemin güvenliği için gerekli bir adımdır. bu nedenle oy sayım programı bütün oyları indirerek sayımı yapar.

6. SONUÇ VE ÖNERİLER

Tez çalışmasında blokzinciri teknolojisi kullanılarak, çevrimiçi bir oylama sisteminin yapılma teknikleri, bunun için gerekli olan kriptolojik protokoller incelenmiş ve örnek bir uygulama geliştirilmiştir.

Bu çalışmada Multichain adında açık kaynak kodlu bir blokzinciri yazılımı kullanılmıştır. Bu sayede madenciler arasındaki rekabete dayalı bir güvenlik mekanizmasına sahip, merkezi olmayan bir veri depolama sistemi elde edilmiştir. Bu bir seçim sisteminin sahip olması gereken en önemli özelliklerden birisidir. Blokzinciri teknolojisi sayesinde oy sayımının herkes tarafından doğrulanabilmesi sağlanmıştır.

Çalışmada oluşturulan oy verme modelinde; sıralı madencilik yöntemi kullanılmıştır. Bu sistemde madencilik yapabilecek taraflar önceden belirlenmiştir. Madencilerin açık anahtarları sistemin bir parçasıdır. Madenciler kendi gizli anahtarlarını kullanarak blokları imzalayabilirler. Madencilerin açık anahtarları ve yetkilendirme sunucusunun açık anahtarları oy kullanmak için kullanılan istemci yazılımın bir parçasıdır. Bu nedenle istemci yazılımın değiştirilmediğinin doğrulanması çok önemlidir. Blokzinciri bu sistemde oyların dağıtık olarak ve güvenli bir şekilde toplanabilmesini sağlamıştır.

Sistemde kullanılan oylar yetkilendirme servisi tarafından dijital olarak imzalanmaktadır. Bu servis seçmenin kimliğini doğrulamaktadır. Bu sayede sadece oy kullanma hakkı bulunan kişiler oy kullanabilir ve sadece bir kere oy kullanabilir. Yetkilendime servisi kör imzalama tekniği ile imzalama işlemi yaptığı için kullanılan oylar yetkilendirme servisinden de gizli kalmaktadır. İstemci yazılım oy kullanmadan önce oluşturduğu özel bir sayıyı yetkilendirme sunucusuna gönderir. Ama göndermeden önce bu sayıyı özel bir gizleme işleminden geçirir bu sayede yetkilendirme sunucusu yetkilendirdiği kişiyi bilmesine rağmen, imzaladığı sayıyı göremez. Daha sonra bu sayıyı özel bir çözümleme işleminden geçirir ve sonuç olarak yetkilendirme sunucusu tarafından imzalanmış ama içeriğinin sadece oy kullanma yazılımı tarafından bilindiği bir değer oluşmuş olur. Bu oluşan sayı oy kullanmak için kullanılır. Bu sayede seçmenin kimliğinin gizliliği ihlal edilmemiş olur.

Kurulan sistemde ayrıca seçmenin IP adresi gibi seçmenin kimliğinin tespit edilmesine imkan sağlayacak bilgilerin, tespit edilememesi için de özel bir protokol geliştirilmiştir. Bu protokol ile oylar, oy toplayıcılar arasında şifreli olarak dolaştırılması sağlanmıştır. Bu protokol sayesinde oylar rastgele seçilen madencilerin açık anahtarları ile şifrelenecek ve bu oyun bu madenciler arasında dolaştırılması sağlanacaktır. Burada seçilen bütün madenciler anlaşmalı olmadığı sürece seçmenin kimliği gizlenmiş olacaktır. Madenciler arasında belli bir rekabet ortamının var olduğu kabul edilirse, bu durum bir güvenlik tehdidi oluşturmayacaktır.

Kurulan sistem ile oy kullanımının ve sayımının güvenliğinin kabul edilebilir düzeyde olduğu bir sistem oluşturulmuştur. Ama İnternet üzerinden yapılacak bir seçim sisteminin güvenliği oldukça dikkat edilmesi gereken ve çok fazla saldırıya veya hileye açık bir konudur. Blokzinciri teknolojisi tek başına bu güvenliği sağlayamaz. Blokzinciri sadece merkezi kontrol noktasını ortadan kaldırır. Bu nedenle ek protokollere ihtiyaç vardır.

Bu çalışma sonucunda çevrimiçi bir oylama sisteminin güvenliğinin sağlanmasının ne kadar zor olduğu anlaşılmaktadır. Tamamen güvenli bir sistem oluşturulabilmesi için bu alanda daha fazla çalışma yapılması gerektiği ortadadır.

KAYNAKLAR

Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timón J., Wuille P., 2014, Enabling Blockchain Innovations with Pegged Sidechains, https://blockstream.com/sidechains.pdf

Barnes, A., Brake, C., Perry, T., 2017, https://www.economist.com/sites/default/files/plymouth.pdf

Bitcongress, 2016, https://bravenewcoin.com/assets/Whitepapers/BitCongressWhitepaper.pdf

BitFury Group, 2015, Proof of Stake versus Proof of Work, 2015.

BitPay., 2015, Inter-Channel Payments: Impulse, http://impulse.is/impulse.pdf

Buterin V., 2014, A Next-Generation Smart Contract and Decentralized Application Platform, https://github.com/ethereum/wiki/wiki/White-Paper

Castillo, M., 2018, https://www.coindesk.com/russias-capital-leading-charge-blockchain-democracy

Chaum, D., 1983, Blind signatures for untraceable payments.

Courtois N. T., 2014, On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies, http://arxiv.org/abs/1405.0534.

Decker C., Wattenhofer R., 2014, A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels, Distributed Computing Group, ETH Zurich.

Evans D. S., 2014, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms, Coase-Sandor Inst. for Law & Economics Work. Paper No. 685.

Followmyvote, 2017, https://followmyvote.com

Hao, F., Ryan, P.Y.A., 2016, Real-World Electronic Voting: Design, Analysis and Deployment, Chapter 7, Auerbach Publications, ISBN:9781498714693.

Kettley, S., 2017, Vote online: Can you vote online in the General Election 2017?, www.express.co.uk/news/politics/814685/Vote-online-election-2017-can-you-vote-online-UK-general-election

King S., Nadal S., 2012, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, https://ia601705.us.archive.org/33/items/PPCoinPaper/ppcoin-paper.pdf

Lamport L., 1978, Time, Clocks, and the Ordering of Events in a Distributed System", Communications of the ACM : 21 / 7, 558-565.

Lowe, J., 2017, Netherlands Abandons Electronic Vote Counting Amid Hacking Fears, Newsweek.

Nakamoto S., 2009, Bitcoin: A Peer to peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

Pennetier, M.L., Thomas, L., Stonestreet, J., 2017, France drops electronic voting for citizens abroad over cyber security fears, Reuters.

Polys, 2017, https://polys.me/

Poon J., Dryja T., 2015, The Bitcoin Lightning Network, https://lightning.network/lightning-network-paper.pdf

Scytl Online Voting, 2015, Online Voting Technology, www.scytl.com/wp-content/uploads/2015/09/DIGITAL_online-voting.pdf

Shamir, A., 1979, How to share a secret, Communications of the ACM, 22 (11): 612–613.

Sompolinsky Y., Zohar A., 2014, Accelerating Bitcoin’s Transaction Processing, https://eprint.iacr.org/2013/881.pdf

Szabo N., 1997, Formalizing and Securing Relationships on Public Networks, First Monday, (http://szabo.best.vwh.net/formalize.html), Volume 2, Number 9.

Todd P., 2014, Near-zero fee transactions with hub-and-spoke micropayments, http://sourceforge.net/p/bitcoin/mailman/message/33144746/

Wood G., 2015, Ethereum: A Secure Decentralized Generalized Transaction Ledger, http://gavwood.com/Paper.pdf

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı **:** Muhammed Emin Aydın

Uyruğu **:** Türk

Doğum Yeri ve Tarihi: Iğdır, 01.11.1989

Telefon **:** 0506 977 1324

Fax **:**

Email **:** muhammedemin.aydin@ogr.konya.edu.tr

EĞİTİM

Derece	**Adı, İl**	**Bitirme Yılı**
Lise	: Kırıkkale Cumhuriyet Yabancı Dil Ağırlıklı Lisesi	2007
Üniversite	: Selçuk Üniversitesi, Bilgisayar Mühendisliği, Konya	2012
Yüksek Lisans	:	
Doktora	:	

İŞ DENEYİMLERİ

Yıl	**Kurum**	**Görevi**
2014 - 2018	Euromessage Çok Kanallı Pazarlama	Yazılım Mühendisi
2018 - Devam	Whitehorse Yazılım	Yazılım Mühendisi

UZMANLIK ALANI

- **Programlama Dilleri:** C/C++, Python, Javascript, Go, Rust
- **İşletim Sistemleri:** Linux, Windows, Android

YABANCI DİLLER

- **İngilizce**