Blokzincir Tabanlı E-seçim Sistem Önerilerinin Güvenlik ve Mahremiyet Analizleri

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

Latif Anıl BÜYÜKBASKIN

tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

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

ONAYLAYANLAR:

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

Dr. İsa Sertkaya
(Tez Eş-danışmanı) .....

Prof. Dr. Nizamettin Aydın .....

Dr. Mehmet Serkan Apaydın .....

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

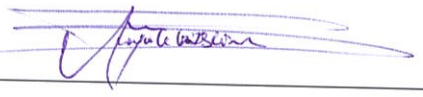
ONAY TARİHİ: 29.08.2019

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Latif Anıl Büyükbaskın, başlığı, 'Blokzincir Tabanlı E-seçim Sistem Önerilerinin Güvenlik ve Mahremiyet Analizleri' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

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

İmza: 

Tarih: 29.08.2019

Security and Privacy Analysis of Blockchain-based E-voting Schemes

Latif Anıl Büyükbaskın

Abstract

Today, developing technology is one of the most effective tools to make our lives easier. Although blockchain technology is a new era in e-voting subject, it is thought that it can play a key role in solving many critical problems. Therefore, the applicability of blockchain-based e-voting systems is being researched.

In this thesis, based on the requirements and features that an e-voting systems should fullfill are defined by Popoveniuc et al., Fujioka et al., Cranor et al., Benaloh et al., Juels et al. and Çetinkaya et al. The selection of blockchain-based e-voting systems that have been proposed so far in the light of these requirements, eligibility, uniqueness, forgiveness, robustness, fairness, privacy, coercion resistance, receipt freeness and end-to-end verifiability are analyzed. As a result of these analyzes, it has been determined that a mature blockchain based e-voting system that can meet all criteria has not been proposed yet. In addition to these analyzes, time and cost analysis of block chain based e-voting application was made based on national elections in Turkey.

Besides the advantages and potential of blockchain technology within the scope of e-voting, possible new threat elements are mentioned. Accordingly, the availability of blockchain-based e-voting has been discussed, and it has been shown that it would be more advantageous to move to e-voting specific blockchaining technologies over cryptocurrencies.

Keywords: E-voting, privacy, blockchain

Blokzincir Tabanlı E-seçim Sistem Önerilerinin Güvenlik ve Mahremiyet Analizleri

Latif Anıl Büyükbaskın

Öz

Günümüzde gelişen teknoloji hayatımızı kolaylaştırmak adına en etkili araçlardan biridir. Bu alanlardan biri olma yolunda ilerleyen blokzincir teknolojisi elektronik seçim yöntemleri konusunda yeni bir dönem olmak ile beraber, kritik bir çok problemin çözümü konusunda kilit rol oynayabileceği düşünülmektedir. Bu nedenle blokzincir tabanlı e-seçim sistemlerinin uygulanabilirliği araştırılmaktadır.

Bu tez çalışmasında, e-seçim sistemlerinin sağlaması gereken gerek ve özelliklerin Popoveniuc vd., Fujioka vd., Cranor vd., Benaloh vd., Juels vd. ve Çetinkaya vd. tarafından yapılan çalışmalara dayalı olarak derlemesi yapılarak, şu ana kadar önerilmiş blokzincir tabanlı e-seçim sistemlerinin bu gerekler ışığında seçme hakkının sağlanması, emsalsizlik, bağışlayıcılık, dayanıklılık, adillik, mahremiyet, baskı dirençliliği, makbuzsuzluk ve uçtan uca doğrulanabilirliklerinin analizleri yapılmaktadır. Bu analizler sonucunda tüm kriterleri karşılayabilen olgunlaşmış bir blokzincir tabanlı e-seçim sisteminin henüz önerilmediği tespit edilmiştir. Bu tespitler aynı zamanda Türkiye genel seçimleri baz alınarak, ülke çapında geniş katılımlı bir seçimde blokzincir tabanlı e-seçim uygulamasının süre, maliyet analizi yapılmıştır.

Bu sonuçların yanısıra blokzincir teknolojisinin e-seçim kapsamında getirdiği avantajlar ve potansiyelin yanısıra, olası yeni tehtid unsurlarına ve buna bağlı olarak blokzincir tabanlı e-seçim hazır bulunurluğu tartışılmış, kriptoparaların üzerinde bir e-seçim yerine e-seçime özgü blokzincir teknolojilerine yönelmenin daha avantajlı olacağı görülmüştür.

Anahtar Sözcükler: E-seçim, mahremiyet, blokzincir

Teşekkür

Her zaman sağlamış oldukları maddi ve manevi destekleri için ailem başta olmak üzere, bana burs imkanı sağlayan kurumum TÜBİTAK Marmara Araştırma Merkezi'ne, bu tez çalışmasına önderlik edip sağlamış olduğu destekler için sayın hocam Dr. İsa Sertkaya'ya, kritik yönlendirmeleri ve tavsiyeleri için Prof. Dr. Ensal Gül'e teşekkürlerimi sunarım.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

SBİ **S**ıfır **B**ilgi **İ**spatı

ÖBK **Ö**n ödemeli **B**itcoin **K**artı

DRE **D**irect **R**ecording **E**lectronic

Bölüm 1

Giriş

Seçim, toplumların oy kullanarak ortak bir karara varmasının resmi sürecidir. Demokrasinin insan hakları çerçevesinde gereği olarak seçimlerin yapılma yöntemi özgür iradeye dayanmalıdır. Bu nedenle, seçimlerin yapılış formatı ile özü arasındaki farkı ayırt etmek önemlidir, [1]. Bazı durumlarda, biçimsel olarak seçim yapılırken, gerek seçmenlerin özgür olarak düşüncelerini ifade etmelerini engelleyebilecek meseleler olsun, gerek en az bir alternatifin sunulmayışı olsun seçim yapmanın özünü gözden kaçırılabilmektedir. İnsanların kararlarını herhangi bir baskı altında kalmadan yansıtabilecekleri bir seçim sistemi aracılığı ile ortak bir karara varılabilmesi için söz konusu olan seçim sisteminin özgür ve çoğulcu bir ortamda genellik, eşitlik ve gizlilik kriterlerini sağlaması gerekmektedir.

Geleneksel kağıt tabanlı seçim sistemleri günümüzde en yaygın kullanılan seçim sistemi türüdür. Seçmenin tercihini bir kabin içerisinde işaretlediği kağıt tabanlı seçim sistemleri seçme hakkı ile birlikte seçmen gizliliğini sağlayan en basit yöntemdir. Seçimde oy kullanabilecek özellikleri sağlayan seçmenler belirlenerek, oy kullanacak seçmen listeleri seçimden önce duyurulur. Uygun seçmen listesi, Türkiye özelinde silâhaltında bulunan askerler, askeri öğrenciler ve ceza infaz kurumlarında hükümlü olarak bulunanlar hariç tutularak 18 yaşını doldurmuş her Türkiye Cumhuriyeti vatandaşı oy kullanabilir olarak belirtilmiştir, [2]. Kağıt tabanlı seçim sistemlerinin en önemli özelliklerinden biri seçmenlerin oyunu kabin içerisinde kullanması ile sağlanan mahremiyettir. Burada sağlanmakta olan mahremiyet bir takım özellikleri beraberinde barındırmaktadır. Kabin içerisindeki

bir seçmenin çevresi ile olan açık ve gizli tüm iletişim kanallarının kapatılmasından dolayı oy kullanma aşamasında bir seçmenin potansiyel baskı kaynaklarından ayrı tutulması ile seçim sistemi baskı dirençliliği özelliği de göstermektedir, [3]. Bunun yanı sıra, bir seçmen kullanmış olduğu oyu ispatlamasının doğrulanabilir kesin bir yolu bulunmaması seçmenin özgür tercihini baskı veya oy ticareti gibi gerçek tehtidlere karşı korunmasını sağlamaktadır, [4]. Seçim sonuçlarını sandıklar açılmadan elde etmek mümkün olmadığı için her oy kullanan seçmen için adil bir ortam oluşturularak kararlarının diğer seçmenlerin tercihlerinden etkilenmeleri mümkün değildir, [5]. Tüm bu özellikler ve fazlası geçmişten günümüze tecrübe ile gelişerek adil bir seçim sürecinde oy kullanılabilmesi için evrilmektedir.

Kağıt tabanlı seçim sistemlerinin sağladıkları özellikler ile birlikte dezavantajları da bulunmaktadır. Her bir seçmen kullanmış olduğu oyun sayımlarda sayıldığından emin olabilmesi için oyunu doğrulayabilmesi gerekmektedir. Kağıt tabanlı seçim sistemlerinde doğrulanabilirlik için sunulan öneriler [6–8] bulunmaktadır. Ancak bu çözümler kağıt ve personel maliyetlerini azaltmak adına bir çözüm sağlamamaktadırlar. Oy kullanma ve sayım işleminin doğrulanabilir olmamasından dolayı ortaya çıkabilecek potansiyel insan hataları ve sahtekarlıklar seçimin bütünlüğünün sağlanamamasına neden olmaktadır. Mevcut sistemlerde, gerekli görülen önlemler alınmış olsa dahi, bu çözümler yeterli olmamaktadır. Tüm bu olumsuzlukların yanı sıra, her bir seçim için karşılanması gereken kağıt maliyeti hem doğaya hem de ekonomiye ağır bir yük oluşturmaktadır. Kağıt masrafının yanı sıra seçimlerde görevlendirilecek personelin eğitilmesi ve görevlendirme karşılığında ödenen ücretler, oy kullanma noktalarının oluşturulması da dahil edilirse ülke çapında gerçekleştirilmek istenen bir seçim için oluşturulması gereken bütçe gittikçe artmaktadır, [9]. Bu bütçenin her seçim için tekrardan oluşturulması gerekmektedir.

Elektronik seçim (e-seçim) oy kullanımının veya oy sayımı için elektronik cihazlarının yardımı ile yapıldığı oylama çeşitidir, [10]. Temel olarak e-seçim türleri iki ana çeşitte belirtilebilir. Bunlardan ilki, temsilcinin fiziksel olarak seçim görevlileri tarafından denetlenen seçim istasyonlarında elektronik cihazlar aracılığı ile oy kullanıldığı direkt kayıt e-seçim (DRE) yöntemidir. Diğer yöntem ise internet aracılığı ile seçmenlerin kendi elektronik cihazları ile uzaktan oy kullanması şeklinde denetlenmeden gerçekleştirilen internet e-seçim (i-voting) türüdür.

İlk olarak David Chaum[11] tarafından ortaya atılması ile beraber, elektronik seçim

sistemleri üzerine tasarım ve analizler günümüzde de halen yoğun bir şekilde çalışılan bir araştırma konusudur, [12–16]. Modern dünyada dijitalleşme yolunda atılan adımlardan biri olarak e-seçim sistemleri, demokrasiye giden yolda büyük engellerden olan seçim maliyetleri azaltılması, uzaktan oylama imkanı sağlanarak seçim günü sandığa gidemeyen seçmenlerin katılımı ile birlikte seçime olan katılımın arttırılması ve seçmenlerin kullandıkları oyların seçim sonunda yapılan sayıma olan etkisinin doğru bir şekilde etkilediğinin doğrulanabilmesi, insan hatalarından veya olabilecek sahtekarlıklardan kaynaklanabilecek hataların tespiti ile daha güvenilir ve şeffaf seçim süreçleri ortaya koymak hedeflenmektedir. Ayrıca sayım hızı arttırılarak seçim sonuçlarının daha kısa sürede yayınlanabilmesi istenilen özelliklerdendir. Yapılan bir araştırmaya [17] göre oylama ve sayım prosedürünün seçmenin mahremiyetini bozmayacak şekilde şeffaf olması seçim sonucuna olan güveni arttırmaktadır. Ayrıca bir başka araştırmaya [18] göre seçim günün seçmenlerin harcadıkları efor ve zaman azaldıkça seçimlere katılım oranının arttığı gözlemlenmiştir.

Uzaktan e-seçim sistemleri beraberinde getirdikleri teknoloji ve potansiyel kolaylıklar ile beraber bazı problemlerin de ortaya çıkmasına neden olmuştur, [19]. E-seçim gereksinimlerinin karşılanması bankacılık veya e-ticaret gibi diğer çevrim içi servislere nazaran karşılaştırıldığında doğasından kaynaklanan zor bir denge problemidir. Bir yandan seçmen mahremiyetinin sağlanması gerekirken, diğer tarafdan kullanılan oyların, oy kullanma hakkı bulunan seçmenler tarafından kullanıldığının ve doğru formatı sağladıklarının açık olarak herkes tarafından doğrulanabilmesi gerekmektedir. Seçmenlerin kullandıkları oyların seçim sonuçlarına doğru bir şekilde etki gösterdiğinin kendileri tarafından doğrulanabilmesi istenirken, diğer yandan kullandıkları oyları üçüncü kişilere ispatlayabilmelerinin bir yönteminin bulunmaması gerekmektedir.

Günümüzde kullanılan e-seçim sistem tasarımlarının istemci-sunucu mimarisi üzerine kurulu olmasından dolayı verinin bütünlüğünün sağlanması sorumluluğu güvenilir üçüncü partiler tarafından sağlanmaktadır, [20]. Seçimde oy kullanacak seçmenin kimliği ve seçme hakkı için kontrol edilirken seçimde kullandığı oyun tesliminin seçimi yürüten kişiler dahil anonim olarak kimse tarafından takip edilemediğinin ispatlanması bahsedilen problemlerden biridir. Ayrıca merkezi olarak yürütülen bir seçim sisteminde, tekil kırılma noktası olmasından dolayı, tek bir dürüst olmayan otorite yada kişi tarafından tüm seçim verisinin farkedilmeden değiştirilmesi riskini arttırmaktadır. Benzer şekilde tek noksanlık noktasının DDoS ataklarına karşı savunmasız olması nedeniyle seçim süreci

boyunca bilgi güvenliğinin temel kriterlerinden olan ulaşılabilirliğin engellenmesi bir risk olarak karşımıza çıkmaktadır. Yine merkezi bir sistem olmasından dolayı potansiyel olarak oluşabilecek arızalar nedeniyle seçimin bütünlüğünün bozulmasının seçmen ve gözlemciler tarafından takip edilememesidir. Ayrıca, seçimde kullanılacak cihazların üretimi ve kullanımı üzerine güvenlik meseleleri sıkça tartışılan konulardan biridir. Bunların yanı sıra e-seçim sistemlerinin endişe sebepleri, sistemlerin açık kaynak olmaması, öyle olsa bile sunucularda yürütülen süreçlerin bilinmiyor olması, seçimi yürüten otoritelerin gereğinden fazla güçlü konumda bulunmaları [21] problemlerden bazıları olarak gösterilebilir.

Günümüzde e-seçim sistemleri Brezilya [22], Estonya [23], İsviçre [24], ABD [25], Norveç [26], Kanada [27] ve Avustralya [28] gibi bazı ülkeler tarafından denenmiştir ve bazıları hala kullanılmaktadır. Bu sistemlerin güvenliklerinin yeterliliği hali hazırda literatürde tartışılmaktadır. Örneğin yakın zamanda İsviçre'de yapılan bir yarışma sırasında kullanılan e-seçim sisteminde saldırgan tarafından kullanılan oyların farkedilmeden değiştirebilmesi bir kusur olarak ortaya çıkarılmıştır, [29]. Springall vd., Estonya tarafından hala kullanılmakta olan internet e-seçim sistemi üzerine yaptıkları çalışmada güvenlik analizleri sonucunda devlet düzeyinde saldırgan, sofistike suçlu veya dürüst olmayan bir sistem yöneticisinin seçim sonuçlarını manipüle etmek için hem teknolojik hem de prosedürel kontrolleri aşabileceğini göstermişlerdir, [30]. Bir başka çalışmada, Aranha vd. tarafından Brezilya e-seçim sistemi güvenliği analizi yapılmıştır. Seçim yazılımının minimum güvenlik kriterlerini sağlamadığı ve sistemin kapalı kaynak yazılım kullanımı başta olmak üzere şeffaflık üzerine olgunlaşmamış olması tartışılmaktadır, [31].

Mevcut olarak kullanılmakta olan seçim sistemi yerine e-seçim sistemlerinin kullanılabilmesi için sunulan sisteminin en az mevcut sistemin sağlamakta olduğu kriterleri yerine getirmesi gerekmektedir. Bir e-seçim sisteminin kullanılabilmesi için gerekli kriterler literatürdeki çalışmalarda [3–5, 32–34] ortaya konulmuştur. Özellikle uçtan uca doğrulanabilirlik konusunda Popoveniuc vd. tarafından yapılan çalışma [34] bir seçmenin tüm seçim sürecleri arasında doğrulayabilmesi gereken konuları açık olarak belirtmiştir. Uçtan uca doğrulanabilir seçim teknikleri, bir seçmenin bireysel olarak seçimi oluşturan kritik yapıları seçim yazılımı, yetkilileri, donanımı veya prosedürlerine güvenmesi gerekmeksizin kontrol edilebilmesini sağlayabilmesi için gerekli görülen özelliklerdir, [35]. Elektronik oylama sistemleri ile maliyetlerin azaltması, seçmen katılımını arttırılması, seçim sonuçlarının doğrulanmasının yapılabilmesi istenirken, beraberinde gerçek hayatta

karşılaşılabilecek oy satın alma, seçmen baskısı yada kullanılan oy pusulasının iptal ettirilmesi gibi sistemin kötüye kullanımını riskini arttırmaktadır.

Satoshi Nakamoto rumuzu altında, 2008 yılında yayınlanan Bitcoin [36] kripto parası ile ilk kez internet üzerinde birbirine güvenmeyen aktörler arasında, güvenilir üçüncü bir kişiye ihtiyaç duyulmaksızın, değer transferi yapılması mümkün kılınmıştır, [36]. Bitcoin kripto parasında değer transferinin yapılmasını sağlayan yapı ise blokzincir olarak adlandırılan dağıtık, kriptolojik olarak güvenli, sadece eklenebilir olarak değiştirilebilen şeffaf bir veri yapısı ile sağlamaktadır. Bir mutabakata bağlı olarak birbirinin ardına eklenen bloklar, sistem üzerinde gerçekleşen ilgili aktarımların depolanması işlevini, verilerin bütünlüğünün bozulmasına müsade etmeyecek şekilde, üstlenen kayıt defterin oluşmasını sağlamaktadır. Bitcoin kripto para olarak adlandırılan değerlerin trasferinin yapılabildiği bir finansal yapı olarak düşünülebilirken, blokzincir aktörler arası merkezi olmayan, şeffaf bir kayıt mekanizması olarak düşünülebilir. Blokzincir teknolojisi, bu anlamda kripto paralardan daha geniş kapsamlı bir anlam ifade etmektedir.

Nispeten yeni gelişen blokzincir teknolojisi, yapısının dağıtık olması, veri bütünlüğünün şeffaf olarak herkes tarafından doğrulanabilir olması, inkar edilemeyecek şekilde daha önceden eklenmiş verinin değiştirilememesi gibi özellikleri sağlamasından dolayı birçok alanda çözüm olarak önerilmeye başlanmıştır. Bu alanlara örnek olarak yardım kuruluşlarına yapılan bağışların takibinin yapılmasını sağlamak [37, 38], tedarik zincirleri takibinin RFID kullanılarak takibinin yapılması [39–41], sağlık sigorta hizmetlerinde kişilerin kendi sağlık bilgilerinin kontrolünün sağlanması ile daha verimli hizmetlerin oluşturulması [42, 43], telif haklarının düzenli olarak sanatçıdan direkt olarak tüketiciye ulaştırılması ve takibinin sağlanması [44, 45], nesnelerin interneti (IoT) alanına dağıtık olarak çalışan çok miktarda cihazın güvenli olarak yönetiminin sağlanması [46–48] gibi birçok alanda blokzincir kullanımı son yıllarda tartışılan bir ilgi odağıdır. Bu gelişmelere ve çalışmalara paralel olarak, bu uygulamalardan biri olarak blokzincir tabanlı e-seçim sistem tasarımı önerileri göze çarpmaktadır.

Geleneksel metodlar ile çözüm üretiminde zorlanılan gereksinimler göz önüne alındığında, blokzincir teknolojisinin sağlamakta olduğu özelliklerin e-seçim sistemleri için ümit vadettiği düşünülmektedir. Mutabakat mekanizmaları sayesinde seçimi yürüten şahısların veya kurumların seçim süreçleri üzerindeki gücünü kısıtlayarak süreçlerin dağıtık olarak daha şeffaf ve güvenilir bir biçimde yürütülmesine olanak tanıyacağı düşünülmektedir. Bunun

yanı sıra, mutabakat mekanızmasının çalışabilmesi için gerekli olan değiştirilemez defter yapısı, bir seçmenin oyunun kayıt ettirdikten sonra emanet zinciri (chain of custody) gibi üçüncü bir yapıya güvenmesi gerekmeksizin pusulasının üzerinde oynanmadığından emin olabilmesini sağlayacağı düşünülmektedir. Sağlanması zor olduğu düşünülen bu problemin yayınlanan bir çok makalede potansiyel çözümün blokzincir teknolojisi ile kalıtsal olarak gelen özelliklere dayalı olarak sağlanabileceğinden bahsedilmektedir. Wüst vd. tarafından yayınlanan çalışmada gereksinimleri ve dengeleri göz önüne alındığında blokzincir teknolojisinin kullanımının makul olabileceği belirtilmiştir, [49].

E-seçim sistemlerinde blokzincir kullanımı geleneksel sistemlere göre birçok avantaja sahip olmasıyla birlikte farklı problemlere de sahiptir. Özellikle, temsili demokrasinin temel yapı taşlarından biri olan seçme hakkının güvenli bir şekilde sağlanması gibi kritik öneme sahip bir konuda teknolojinin sagladığı kolaylıkların yanı sıra beraberinde getirdiği problemlerin de mutlaka sorgulanması gerekmektedir.

İlgili Çalışmalar Yayınlanan başlıca blokzincir tabanlı e-seçim önerileri özet yapıları ile birlikte liste halinde belirtilmiştir.

- Zhao vd. tarafından 2015 yılında ilk blokzincir tabanlı e-seçim sistemi [50] önerilmiştir. Bitcoin kripto parasının üzerine zk-SNARK [51] ile seçmenin davranışına göre ödül/ceza vererek oy sistemi tasarlamışlardır.

- Cruz vd. tarafından 2017 yılında Bitcoin kripto parası kullanılarak kör imzalama ve ön ödemeli Bitcoin kartları ile bir e-seçim sistemi önerilmiştir, [21].

- Tarasov vd. tarafından 2017 yılında ZCash kripto parasının mahremiyet özelliklerinden faydalanan ancak merkezi bir sunucu ile organize edilen bir e-seçim sistemi önerilmiştir, [52].

- Yifan Wu vd. tarafından 2017 yılında Bitcoin kripto parası ve halka imzaları kullanarak anonimliği sağlayan bir e-seçim sistemi önerilmiştir, [53].

- Yi Lui vd. tarafından 2017 yılında e-seçim için tasarlanan özel bir blokzincir ağının tasarlanarak, mahremiyetin kör imzalar ile sağlandığı bir e-seçim sistemi önerilmiştir, [54].

- McCory vd. tarafından 2017 yılında Ethereum blokzinciri üzerinde akıllı sözleşmeler ile az sayıda ve birbirini tanıyan katılımcılar göz önünde bulundurularak tasarlanmış maksimum seçmen mahremiyeti sağlayan kendiliğinden sonuçların sayıldığı bir e-seçim sistemi önerilmiştir, [55].

- Ticari olarak e-seçim hizmeti sağlayan Poly's Online Voting, Ethereum blokzinciri üzerinde akıllı sözleşmelerin yardımı ile ElGamal algoritmasının homomorfik özellikleri ile sıfır bilgi ispatından yararlanılarak geliştirilmiştir, [56].

- Ayed vd. tarafından 2017 yılında konsept olarak her bir adayın kendi blokzincirine sahip olduğu özet fonksiyonlarına dayalı geleneksel seçim yöntemlerine nazaran daha dağıtık bir yapıda e-seçim sistemi önerilmiştir, [57].

- Baocheng Wang vd. tarafından 2017 yılında geniş ölçekli seçimlerde kullanılmak üzere Ethereum blokzinciri üzerinde homomorfik ElGamal ve halka imzalarından faydalanarak bir e-seçim sistemi önerilmiştir, [58].

- Hardwick vd. tarafından 2018 yılında, blokzincir teknolojisini sandık olarak kullanan potansiyel bir e-seçim sistemi önererek, e-seçim sistemleri için blokzincir kullanımının avantajları ve dezavantajları tartışılmıştır, [59].

- Hjalmarsson vd. tarafından 2018 yılında geniş ölçekli seçimlerde kullanılmak üzere blokzincir tabanlı e-seçim sistemi önerilmiştir, [60].

- Khoury vd. tarafından 2018 yılında Ethereum blokzinciri kullanılarak akıllı sözleşmeler ve SMS ile kimlik doğrulama tabanlı bir e-seçim sistemi önerilmiştir, [20].

- Adiputra vd. tarafından 2018 yılında ortak seçim anahtarı kullanarak blokzincir tabanlı bir e-seçim sistemi önermişlerdir, [61].

Cucurull vd. tarafından 2019 yılında, blokzincir tabanlı bazı e-seçim sistemlerinin [56, 62–67] Avrupa Birliği tarafından genel olarak önerilen e-seçim kriterlerine göre uygunluklarının karşılaştırması incelenmiştir. Yapılan çalışma sonucunda blokzincir tabanlı seçim sistemlerinin araştırma yapılması ile beraber uzun vadede seçmen mahremiyetinin ifşasına neden olabilicek risk faktörlerine dikkat çekmişlerdir, [68].

Zhao vd. tarafından önerilen sistem, Bitcoin üzerinde dağıtık bir piyango gibi seçmeni davranışına göre ödüllendiren ya da cezalandıran sadece iki adaylı bir seçim sistemi önermişlerdir, [50]. Eğer seçmen beklenildiği gibi davranış sergilemez ise sisteme yatırdığı

parayı kaybetmektedir. Ayrıca betikler Bitcoin betikleri ile gerçekleştirilmesinden dolayı protokol seçim kurallarının değişimine karşı esneklik gösterememektedir. Ayed vd. tarafından önerilen sistem, diğer blokzincir yaklaşımlarından farklı olarak her aday için bir zincir üretilmesini önermektedir, [57]. Sistemde seçmenler kendi anahtarlarını oluşturmamakta, transfer işlemleri yerine oy kullanabilmek için blok oluşturmaları gerekmektedir. Üretilen bloklar içerisinde kimlik bilgileri ile birlikte kendilerine verilen seçmen ID'lerinin özetleri bulunmaktadır. Ancak üretilen zincirlerde kullanılan mutabakat, seçmenler tarafından oluşturulan blokların doğrulanması gibi detaylar hakkında bir bilgi bulunmamaktadır. Hardwick vd. tarafından önerilen e-seçim sistemi izinli blokzincir altyapısını kullanarak akıllı sözleşmeler üzerinde adillik, seçmen uygunluğu, mahremiyet ve doğrulanabilirlik kriterlerini sağladıklarını iddia etmektedir, [59]. Ancak, seçim otoritesinin seçmen kimliği ile kullandığı oy arasında bağ kurulabildiğini belirtilmektedir, [69]. Hjalmarsson vd. tarafından önerilen sistem, seçim sonucunu akıllı sözleşmeler ile elde etmektedir, [60]. Hala çalışılmakta olduğu ve sağlanıldığı iddia ettikleri kriterler için henüz test edilmediği belirtilmiştir, [70]. Ayrıca, seçmenlerin seçim süresi boyunca kısmi sonuçlara erişebildiği belirtilmiştir, [71]. Khoury vd. önerilen sistemde oylar seçmen kimlik bilgisi ile birlikte açıktan gönderilmektedir, [20]. Adiputra vd. tarafından önerilen sistemde genel seçim anahtarı ile oylar şifrelenmekte ve seçim sonuçları anahtar yayınlanarak elde edilmektedir, [61]. Çalışmada belirtildiği üzere seçim komitesi, tüm seçmenler ile kullandıkları oylar arasında bağ kurabilmektedir. Bu tez çalışmasında bahsedilen nedenlerden dolayı belirtilen çalışmalar dahil edilmemiştir.

Bilimsel Katkı Bu tez çalışmasında, ilk önce [3–5, 32–34] tarafından yayınlanmış makalelerde tanımlanan e-seçim gerekliliklerine tekrar baktıktan sonra yayınlanan blokzincir tabanlı e-seçim sistem önerilerini [21, 52–56] belirtilen gereksinimleri baz alarak analiz edilmiştir. Yapılan analiz ve değerlendirme sonucunda aşağıda belirtilen bulgular tespit edilmiştir:

- [21] sisteminin, iddia edilenin aksine, adillik ve mahremiyet özellikleri sağlamadığı ve bağışlayıcılık, baskı dirençliliği ve makbuzsuzluk özelliklerini göz ardı ettiği,
- [52] sisteminin seçmen mahremiyetini sağladığı ancak Zcash protokolünün değiştirilmeden kullanılmasından kaynaklanan uçtan uca doğrulanabilirlik, seçmen uygunluğu, emsalsizlik ve dayanıklılığı sağlamadığı,

- [53] sisteminin iddia edilenin aksine dayanıklılık, mahremiyet ve baskı dirençliği sağlamadığı ve bağışlayıcılık özelliğini göz ardı ettiği,
- [54] sisteminin adillik ve mahremiyet özelliklerini sağlamadığı ve bağışlayıcılık, baskı dirençliliği ve makbuzsuzluk özelliklerini sağlamadığı,
- [56] sisteminin baskı dirençliliği ve makbuzsuzluk özelliklerini sağlamadığı ve uzun vadede mahremiyetin açık edilebilme olma risklerinin bulunduğu

Ayrıca, analiz edilen sistemlerin, güvenlik ve mahremiyet zaafiyetleri gözardı edilerek Türkiye genel seçimlerinde kullanılması durumunda oluşabilecek maliyet analizi için kestirim yapılmaya çalışılmıştır. Bu durumda dahi süre, maliyet ve verimlilik analizleri sonucunda hali hazırdaki önerilen blokzincir tabanlı e-seçim önerilerinin bu halleri ile klasik seçim mekanizmasının yerini almaktan uzak olduğu ortaya konmaktadır. Kaldı ki güvenlik zaafiyetleri doğal olarak ekstra maliyet getirecektir.

Bu bilgiler ışığında blokzincir tabanlı e-seçim sistemlerinin hazır bulunurluk analizi verilmektedir. Sonuç olarak blokzincir teknolojilerinin sağlamakta olduğu özelliklerin e-seçim mekanizmaları ile entegrasyonu için bu analizler ışığında daha detaylı çalışmalarının yapılmasının gerektiği ortaya konmaktadır.

Organizasyon Bölüm 2'de seçim kriterleri gözden geçirdikten sonra, bölüm 3'de, blokzincir teknolojisi ve sistemler tarafından kullanılan algoritma ve yapılar açıklamaları ile birlikte bahsedilmekte, bölüm 4'de daha önce belirtilen blokzincir tabanlı e-seçim yayınlarında bulunan güvenlik zafiyetleri sunulmaktadır. Bölüm 5'de hali hazırda bulunan blokzincir teknolojilerinin getirdiği sınırlamaları e-seçim kapsamında tartışılmakla beraber kriterlerin sağlandığı varsayılan bir sistemin Türkiye'de uygulanması halinde karşılaşılacak maliyet ve performans beklentileri belirtilmiştir. En son olarak bölüm 6'de tez çalışması sonucunda elde edilen sonuçlar tartışılmaktadır.

Bölüm 2

E-seçim Sistemi Gereksinimleri

Adil bir seçim ortamı oluşturulabilmesi, seçmen özgürlüğünün sağlanabilmesi ve seçim güvenliğinin sağlanabilmesi için bir seçim sisteminin bazı kriterleri sağlaması gerekmektedir. Bu bölümde [3–5, 32–34] tarafından daha önce tanımlanmış olan gereksinimlere bağlı kalarak, mümkün olacak en kapsamlı gereksinimler kümesini bir araya getirmeye çalışıldı.

2.0.1 Seçme Hakkı (Eligibility)

İnsan hakları evrensel bildirgesinin 21. maddesinde belirtildiği üzere, her bireyin ülkesinin yönetimine doğrudan veya serbestçe seçilmiş temsilciler aracılığıyla ülkesinin yönetimine katkıda bulunma hakkına sahip olduğu belirtilmiştir, [72]. Bu nedenle, kimlikleriyle kayıtlı olan yetkili seçmenlerin oy kullanmalarına izin verilmelidir, [5].

İncelediğimiz tüm e-seçim önerilerinde kayıt otoritesinin seçmenin uygunluğunu değerlendirme sürecinde dürüst olarak davrandığı kabul edilmektedir, bu nedenle bu çalışma kapsamında aynı varsayım devam ettirilmektedir.

2.0.2 Emsalsizlik (Uniqueness)

Bir seçmen, en son sayım sırasında sayılacak en fazla bir oy kullanabilmelidir. Emsalsizliğin seçmenlerin bir defadan fazla oy kullanmasına olanak vermeyen tekrar kullanılamazlık anlamına gelmediğini belirtmek gerekir, [33]. Seçim süreçinde, seçmen birden fazla oy kullanma hakkına sahip olsa bile, sayıma sadece bir oy katkı etmesi gerekmektedir.

2.0.3 Bağışlayıcılık (Forgiveness)

Seçmenlerin oylarını kullanıldıktan sonra tercihlerini oy kullanma süresince değiştirme olanağına sahip olmasıdır. Amaç, geleneksel kağıt tabanlı seçim sistemlerinde kabin ile sağlanan oy kullanma işleminin getirdiği avantajların uzaktan seçim sistemlerinde yoksunluğunu azaltmaktır. Örnek olarak, baskı uygulanarak oyunu kullanmak durumunda kalmış bir seçmene daha sonra kendi oylarını değiştirerek gerçek görüşlerini yansıtabilmesine olanak sağlanabilmesi gösterilebilir. Bu nedenle baskı direnci özelliği ile bağlantılıdır, [33].

2.0.4 Dayanıklılık (Robustness)

Dürüst olmayan katılımcılar tarafından bir seçimin tamamlanmasının ve sonuçun açıklanmasının engellenememesi veya geciktirilememesi gerekmektedir, [5].

2.0.5 Adillik (Fairness)

Henüz oy vermemiş seçmenlerin oylama sırasında oluşan kısmi sonuçların sızmasından dolayı tercihleri etkilenebilmektedir. Tüm seçmenlerin adil şartlarda oy kullanabilmesi için oy kullanımı süreci sona ermeden kısmi sonuçların kimse tarafından elde edilememesi gerekmektedir. Hiçbir şey oy kullanım sürecini etkilememelidir, [5].

2.0.6 Mahremiyet (Privacy)

Seçmenin kimliği ile oy kullanım sırasında beyan ettiği tercihinin arasındaki ilişki hiç kimseye ifşa edilmemelidir.

Bir e-seçimde gizlilik, oylama aşamasında seçmenlerle etkileşime giremeyen bir saldırgan bağlamında tanımlanır, [4]. Seçimi yürüten organizator ile sonuçları sayan kişi anlaşmış olsa bile, seçmen ile oy kullanma arasındaki ilişkiyi tespit edememeliler, [5]. Seçmenin mahremiyeti sonuçların sayımı sırasında korunduğu gibi seçim sonuçları duyurulduktan sonra da gizliliğini korumaya devam etmelidir.

2.0.7 Baskı dirençliliği (Coercion Resistance)

Baskı direnci, saldırganın seçmen ile etkileşime girebileceğinin varsayıldığı, seçmen mahremiyeti özelliğinin daha güçlü bir biçimidir, [4]. Bir saldırgan, bir veya daha fazla seçmeni belirlediği bir aday adına oy kullanması için zorlayabilir veya kullanmış oldukları oyları deşifre etmelerini isteyebilir. Örneğin gizli anahtarlarını açıklamalarını isteyebilir. Eğer saldırgan baskı uygulayacağı seçmenlerin isteği doğrultusunda davranıp davranmadığını ayırt edebiliyorsa, seçmene şantaj yapabilir veya seçim sonucunu yasalara aykırı olarak etkileyebilir.

Baskıya dirençli bir oylama sistemi, seçmenlerin kendi niyetlerine göre oy kullandıkları halde, saldırganı verilen talimata göre davrandıklarını düşündürerek aldatabildikleri bir sistemdir, [4]. Saldırganın hiçbir durum altında seçmenlerin kullandıkları oyun belirtildiği şekilde kullanılıp kullanılmadığını ayırt edememelidir.

Benaloh ve arkadaşlarının belirttiği üzere, seçmenlerin yanlarında potansiyel oy alıcıları veya baskıcı saldırganlar ile birlikte bir seçim protokolüne girmesine izin verilirse, zorlamayı ortadan kaldırmak mümkün olmayacaktır. Bunun nedeni, gerçek bir seçmen pasifken, zorlayıcı bir aracının seçmen rolünü üstlenebilmesidir. Baskıya dirençli bir uzaktan oylama sisteminde, her seçmenin kendi özgür tercihine göre oy kullanabileceği bir an olduğu varsayılır. Bu durumda bir seçim sisteminin baskıya dirençli olabilmesi için seçmenin kendi oyunu değiştirebilmesi olmazsa olmaz bir özelliktir, [3].

2.0.8 Makbuzsuzluk (Receipt-freeness)

Seçmenler ne seçim sırasında ne de seçim bittikten sonra oylarının içeriğini üçüncü bir tarafa ispatlayabilecek bir makbuz elde edememeli veya oluşturamamalıdırlar, [3]. Ancak, Juels vd. tarafından belirtildiği üzere makbuzsuzluk özelliğinin sağlanıyor olması baskı direncliliği özelliğininde sağlandığı anlamına gelmemektedir. Bir saldırgan, seçmenlerden gizli anahtarlarını elde etmeye zorlayarak yada özel anahtarlarını satın alarak da baskı uygulayabilir, [4].

2.0.9 Uçtan Uca Doğrulanabilirlik

Uçtan uca doğrulanabilir seçim teknikleri [34], seçmenlerin bireysel olarak seçim yazılımına, donanıma, seçim görevlilerine veya prosedürlerine güvenmek zorunda kalmadan seçim sonucunun önemli bileşenlerini kontrol edebilmelerini sağlar, [35]. Bir e-seçim sistemi yayınlanan verinin doğrulanabilmesi için bir açık ilan tahtısı bulundurabilir. İlan tahtasında doğrulanacak adımlar uçtan uca doğrulanabilirlik tekniklerinde açıkça belirtilmektedir. Açık ilan tahtası, seçmenler tarafından oluşturulan verinin doğrulanabilmesi için gerekli olmasından dolayı değiştirilemez olacak biçimde sadece eklenebilir olmalıdır. Bir seçimin doğrulanabilirliği, bireysel doğrulanabilirlik ve genel doğrulanabilirlik olmak üzere doğrulayana göre ikiye ayrılabilir.

2.0.9.1 Bireysel Doğrulanabilirlik

Seçmenin kullandığı oyda belirttiği tercihinin seçim sonucu oluşturulurken doğru bir şekilde sayıldığını doğruyabilmesidir. Doğrulanabilir seçim sistemindeki bireysel doğrulanabilirliğin temel gereklilikleri, Popoveniuc vd. [34] tarafından aşağıda belirtildiği gibi tanımlanmaktadır:

Sunulan oy pusulalarının formatının doğruluğu: Seçmenin pusulasında belirttiği tercihin gösterimi ile seçim sistemin geri kalanında kullanılan gösterim seçim sonucuna aynı etkiyi göstermelidir. Seçmen kendisine sunulan pusulanın doğru olup olmadığını tespit edebilmelidir.

Örneğin, Ayşe'nin 1 ve Bora'nın 2 değerlerini kullanarak aday olduğu bir seçimde bir seçmene Ayşe'nin 2, Bora'nın 1 değerleri ile temsil edildiği bir pusula sunulduğunda seçmenin pusulasındaki hatayı seçim sistemine güvenmek zorunda kalmadan tespit edebilmelidir.

Kullanıldığı gibi kayıt: Seçmenin tercihi, seçim sistemi tarafından doğru bir şekilde kayıt altına alınmalıdır. Aksi halde, seçmen oyunun yanlış olarak kayıt edildiğini tespit edebilmelidir.

Bu gereksinim kayıt edildiği gibi sayılma kontrolünün sağlanabilmesi için gerekli olmasının yanı sıra, tutarlılık kontrolü ile birlikte seçmenlerden sayım görevlilerine kadar

olan emanet zincirinin güvenli olduğunu kontrol etmek için de gereklidir. Bir başka deyiş ile kullanılan hiçbir oyun değiştirilmediği ya da silinmediği kontrol edilebilmelidir.

Seçim sisteminin protokolü takip etmesi: Seçim bütünlüğünün sağlanabilmesi için seçmen tarafından seçim sisteminin herhangi bir adımında takip edilen protokolün işleyişinin doğruluğu varsa hataların tespit edilebileceği bir doğrulamanın bulunması gerekir. Eğer sistem protokolü takip etmiyorsa, açık olarak, kabul edilebilir ve reddedilemez bir kanıt sağlanabilmelidir.

2.0.9.2 Genel Doğrulanabilirlik

Herhangi birinin seçim sonucunda oluşan çıktının doğru bir şekilde oluşturulduğunu doğrulayabilmesidir. Doğrulanabilir seçim sistemindeki genel doğrulanabilirliğin temel gereklilikleri Popoveniuc ve arkadaşları [34] tarafından aşağıda belirtildiği gibi tanımlanmaktadır:

Kullanılmış oyların formatının doğruluğu. Seçmenin kullanmış olduğu oy, seçim sonucunu doğru bir şekilde etkilemelidir. Bir oy pusulasu negatif veya fazla oy barındırmamalıdır. Herhangi biri tarafından fazla yada negatif oy barındıran bir pusulanın seçim sonucuna dahil edilmesi tespit edilebilmelidir.

Kayıt edildiği gibi sayılma. Herhangi biri tarafından, yetkililerce duyurulan seçim sonucunun kayıt edilmiş olan geçerli oy pusulalarının tamamından oluşturulduğunu doğrulayabilmelidir. Herhangi biri, tek bir oyun bile sonuça yanlış olarak eklenmesi halinde bu durumu tespit edebilmelidir.

Tutarlılık. Kayıt altına alınan geçerli pusulalar kümesi ile seçim sonucunun hesaplandığı sayılan pusulalar kümesi aynı olmalıdır. Burada emanet zinciri kontrole tabi tutulmaktadır. Eğer iki küme farklı ise, herhangi biri bu durumu tespit edebilmelidir.

Her kayıt edilen oy "kullanıldığı gibi kayıt" kontrolüne tabi tutulmalıdır. Seçim sistemi, bir seçmeni başka bir seçmenin kullandığı oyu kontrol ettirerek kandıramamalıdır. Çünkü bu durum fazladan bir oy pusulanın fark edilmeden sonuçlara eklenebilmesine

olanak tanır. Eğer bir oy pusulanın "kullanıldığı gibi kayıt" doğrulamasını yapabilecek eşsiz bir seçmene sahip olmaması durumunda herhangi biri tarafından bu durum tespit edilebilmelidir.

Doğrulama sırasında bir hata tespit edildiğinde, bu hatanın oluştuğunu belirten bir kanıtının bulunması oldukça arzu edilen bir durumdur.

Yukarıda tanımlanmış olan 'kullanıldığı gibi kayıt' kontrolü hariç tüm kontrollerin açıkca kabul edilebilir ve inkar edilemez kanıtlarının oluşturulabilmesi gerekir. Kanıtların oluşturulamadığı kontroller, *kontrolün zayıf versiyonu* olarak tanımlanmaktadır, [34].

Bölüm 3

Tanımlar ve Notasyon

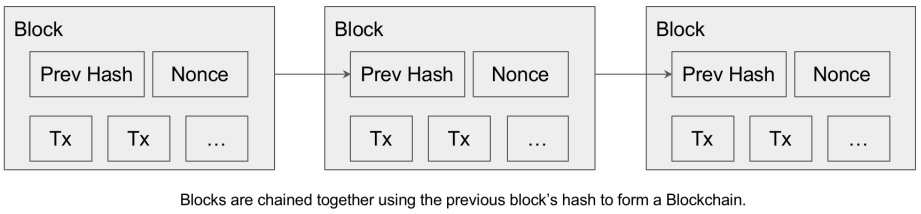
3.1 Bitcoin

Satoshi Nakamoto tarafından 2008 yılında Bitcoin [36] adlı bir kripto paranın yayınlanması ile birlikte blokzincir kavramı ortaya çıkmıştır. Blokzincir, blokların birbirine zincir biçiminde kriptolojik fonksiyonlar ile bağlı olduğu şeffaf, değiştirilemez ve dağıtık bir veri yapısıdır. Blokzincir ile birlikte ilk defa internet üzerinde birbirine güvenmeyen eşler arası, güvenilir üçüncü bir kişiye ihtiyaç duyulmaksızın güvenli olarak değer transferi yapılması mümkün olmuştur.

Blokzincir, bilginin depolandığı blokların ard arda bağlandığı bir kayıt defteridir. Örneğin, Bitcoin eşler arasında gerçekleştirilen transfer işlemleri kayıt altında tutulur. Şekil 3.1'de de görülebildiği gibi her blok kendinden önceki bloğa, bu bloğun özet değerini kendi içerisinde barındırması ile bağlıdır. Bu anlamda bloklar bir zincir formunu almaktadırlar. Oluşturulmuş ilk bloğa başlangıç (genesis) bloğu adı verilir. Diğer bloklardan farklı olarak kendisinden önce bir blok gelmediği için özeldir. Bitcoin kaynak kodlarında görülebildiği üzere Bitcoin başlangıç bloğu The Times gazetesinin 3 Ocak 2009 yılında yayınlanan baskısının başlığı "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" metni ile oluşturulmuş ve önceki blok özet bilgisi sıfır olarak belirtilmiştir, [73]. Herhangi bir bloğun içerdiği veri değiştirildiğinde bloğun özet değeri de değişir. Bu blokzincirin geçerli olabilmesi için kendisinden sonra gelen her bir blokta özet değerlerinin tekrardan hesaplanması gerekmektedir. Mutabakatın şartları yerine

getirildiği sürece, blokların özet değerleri zorluk derecesini sağlayacak biçimde hesaplanmasından dolayı değiştirilemez olarak kabul edilmektedir.

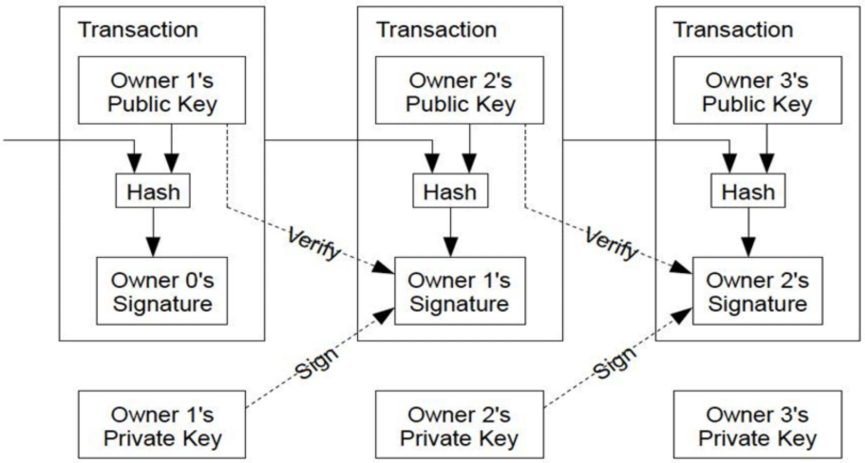
Bloklarda saklanmakta olan tüm transfer işlemlerinin bir araya getirilmesi ile kayıt defteri (ledger) oluşur. Blokzincir ağına bağlı olarak çalışan her düğüm (node), kayıt defterinin bir versiyonunu oluşturmaktadır. Defterler bir anlaşmaya bağlı olarak büyümesi nedeniyle düğümler arasında tekil kalacak biçimde dağıtık olarak senkronize edilmektedir. Bunun sonucu olarak ağ üzerinde işlemler aynı blok sırası ile dizilirler. Bu paranın birden fazla defa harcanmasını engeller.



Şekil 3.1: Blokzincir bloklarının genel yapısı[36].

Transfer işlemlerinin doğrulaması için kriptografik dijital imza algoritmaları kullanılmaktadır, [36]. Bu nedenle blokzincir üzerinde transfer edilebilecek her bir değer bir adrese bağlıdır. Bu adres dijital imzanın açık anahtarı ile üretilir. Şekil 3.2'de gösterildiği üzere değerin sahipliği, üzerinde bulunduğu adrese karşılık gelen gizli anahtara sahip olan kişiye aittir. Değer aktarımı transfer işlemleri ile sağlanmaktadır. Bir transfer işlemi, gönderilen değerin bilgileri ile birlikte alıcısının adresini barındırmaktadır. Değerin sahibi oluşturulan bu yapıyı imzalayarak, alıcıya bu değerin sahipliğinin aktarıldığını belirtmektedir. Transfer işleminin doğruluğunu saylayan mekanizma güvenli imza algoritması olması nedeniyle içeriği değiştirilememektedir veya başkası tarafından imza değeri oluşturulamamaktadır. Transfer edilen paranın geçerliliği üzerindeki ve bağlı olduğu geçmiş transfer işlemlerinin imzaları kontrol edilerek gerçekleştirilir.

Transfer işlemlerinin zincire işlenmesi için imzalanmış işlem blokzincir ağında bulunan düğümlere gönderilir. Her düğüm tarafından alınan işlem bir sonraki düğümlere iletilerek transfer işlemi ağ üzerinde yayılır. Paranın tekrardan harcanamaması (double spending) için ağ üzerindeki düğümlerin bir anlaşmaya vararak transfer işlemlerini belirli bir kurala göre sıralı işlemeleri, bunun sonucunda kendi kayıt defterlerini güncellemeleri gerekmektedir. Bu nedenle bir mutabakata (consensus) varılması gerekmektedir. Mutabakat, bir düğümün kendi kayıt defterini belirli kurallara göre güncelleyerek tüm ağ üzerinde



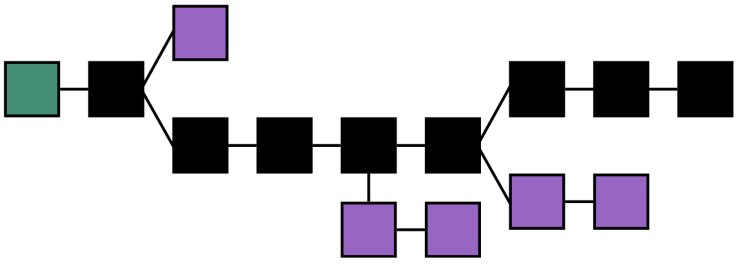
Şekil 3.2: Değerin transfer işlemleri zinciri olarak bulunması[36].

dağıtık olmasına rağmen aynı defterin tutulmasını sağlayan mekanizmadır. Aynı zamanda, transfer işlemlerinin sıralı olarak işlenmesiden ötürü, aynı paranın birden fazla harcanmasının (double spending) önüne geçilmesini sağlamaktadır.

Bitcoin'de mutabakat, işlem gücüne dayanan iş ispatı (proof of work) ile sağlanır. İş ispatına göre, merkezi bir otoriteye güvenmek yerine işlemsel güce güvenilmelidir, [36]. Mutabakatın kurallarından ilki en uzun zincirin düğümler tarafından takip edilmesidir. Zincir üzerinde yeni bir blok oluşturulduğunda, bu blok tüm ağa duyurularak mevcut bulunan geçerli zincire ekleme yapıldığı bildirilir. Her bir düğüm, almış olduğu yeni bloğun doğrulamasını yaparak kurallara uyması halinde kendisinde bulunan defteri günceller. Burada önemli olan noktarlardan biri bloğun oluşturulurken fazla işlem yükü gerektirmesine rağmen, doğrulanmasının hızlı bir şekilde yapılabilmesidir.

Blok üretimi, daha önce belirtildiği üzere belirli kriterleri sağlayacak biçimde bir bulmacaya dayanmaktadır. Bu bulmacayı çözerek blok üretmeye çalışan düğümlere madenci (miner) denir. Her madenci düğüm, ağ üzerinden elde ettiği işlemlerin doğrulamasını yaparak en uzun zincirdeki en son bloğun özet bilgisi ile birlikte üretilmek istenen bloğa eklemektedir. İşlem ispatı mutabakatına göre, oluşturulan bu bloğun özet değerinin bir takım kriterleri sağlıyor olması gerekmektedir. İşlem ispatında oluşturulan bloğun özet değerinin ağ tarafından ortaklaşa belirlenmiş bir zorluk değerine göre ilk n bit değerinin sıfır olması gerekmektedir. Madenciler blok başlığında bulunan tek kullanımlık sayı (nonce) değerini değiştirerek, istenilen kritere uygun bir özet değerine sahip blok aramaya başlarlar. Bu aşamada üç farklı durum gerçekleşebilir. İlk durumda, bir başka

düğüm tarafından bir blok üretilerek en uzun zincir güncellenebilir. Defterin güncellenmesi ile tüm madenciler yayınlanan yeni bloğun doğruluğunu ve sağlaması gereken gereksinimleri kontrol ederek kendi defterlerini güncellerler. Güncellenen deftere göre kendi oluşturmak istedikleri blokların içerisindeki transfer işlemlerini kontrol ederek bloğa eklemek istedikleri transferleri güncellerler. Eğer kendilerinde bulunan bir transfer işlemi bloğa eklenmiş ise bu işlemi kendi üretmeye çalıştıkları bloktan çıkarmaları gerekmektedir. Ayrıca en uzun zincirin en son bloğunun özet değerinin değişmesi nedeniyle oluşturmak istedikleri bloğun önceki özet değeri bilgisini güncelleyerek tekrardan istenilen özellikleri sağlayan bir tek kullanımlık sayı arayışına başlarlar. Bu nedenle bir blok oluşturulduğunda ağ üzerindeki tüm madenciler yeni blok arayışına sıfırdan başlarlar. İkinci durumda, madenci mutabakat gereksinimlerini sağlayan bir blok üretir. Üretilen bu blok diğer düğümlere duyrularak yeni bir blok oluşturulduğu bildirilir. Madenci tarafından bir blok üretildiğinde, blok üretim ödülü (block reward) elde eder. Üçüncü durum ise, birden fazla madencinin birbirine yakın zamanlarda blok ürettiği durumda gerçekleşir. Bu durumda en uzun zincir birden fazla olması nedeniyle, bu eşitlik bozulana kadar düğümler iki bloktan birini seçerek blok üretmeye çalışır. Bu eşitlik bozulduğunda en uzun zincir dışında kalan bloklara yetim blok (orphan block) adı verilir. Yetim bloklara eklenmiş işlemler tekrardan zincire eklenmek üzere yeni oluşturulacak bloklara eklenmelidir. Bu nedenle, blokzincir üzerinde bloğa eklenmiş transfer işlemleri eklendikleri bloktan sonra belirli bir sayıda blok üretilene kadar gerçekleşti olarak kabul edilebilmesi için beklenilmesi tavsiye edilmektedir. Şekil 3.3'de, başlangıç bloğu yeşil, en uzun zincir siyah, yetim bloklar ise mor ile gösterilmektedir.



Şekil 3.3: En uzun zincir ve yetim bloklar[74].

Finansal bir yapı olan Bitcoin'de kullanılan blokzincir mutabakatı başka kurallara da sahiptir. Bunlardan biri zorluk derecesinin 10 dakikada bir blok üretilecek biçimde seçilmesidir. Zorluk derecesinin hesaplanması 2016 blokda bir, yaklaşık iki hafta, ağ üzerinde bulunan düğümlerin hesaplama gücüne göre tekrardan belirlenmektedir. Bu

durum dışında, her bir bloğun saklayabileceği veri miktarının sınırlı olması nedeniyle dakikada işlenebilecek transfer miktarıda sınırlıdır. 210,000 blokda bir, yaklaşık 4 sene, ödül yarıya düşürülerek toplamda üretilen bitcoin miktarının 21 milyon BTC olarak sınırlandırılması sağlanmaktadır.

3.2 Ethereum/Akıllı Sözleşmeler

Bir akıllı sözleşme dijital varlıkların belirli durumlar oluştuğunda aktarılmasını kontrol eden programlardır. Akıllı sözleşme terimi ilk olarak Nick Szabo tarafından 1999 yılında ortaya atılmıştır, [75]. Ethereum makalesinde akıllı sözleşmeler, dijital varlıkların doğrudan gelişigüzel kuralları uygulayan bir kod parçası tarafından kontrol edilmesini içeren karmaşık uygulamalar olarak tanımlanmaktadır, [76]. Ethereum blokzincirinde akıllı sözleşmeler, yığın tabanlı alt seviye baytkod dili olarak Ethereum Sanal Makinası (EVM) tarafından çalıştırılacak biçimde tasarlanmıştır, ancak Serpent gibi yüksek seviye diller ile yazılıp baytkoduna derlenebilmektedir, [77].

Akıllı sözleşmeler iki parti arasında bir anlaşmayı ifade eden programlardır. Blokzincir üzerinde saklanmaları nedeniyle değiştirilemezlerdir. Blokzincir üzerinde çalışan bir akıllı sözleşmede oluşan transfer işlemleri otomatik olarak gönderilebilmektedir. Transfer işlemleri sözleşmede belirtilen şartlar sağlandığında gerçekleşmesi nedeniyle taraflar arasında sözleşmeyi yönetecek üçüncü bir partiye ihtiyaç duyulmamaktadır.

Basit olarak blokzincire kayıt edilmiş bir akıllı sözleşmenin işleyişi kullanıcının sözleşmeye transfer işlemi ile başlar. Transfer işlemi, tüm nodelar tarafından kayıt edilerek sözleşmenin kuralları, yani kodu, verilen parametreler ile çalıştırılır. Sözleşmenin sonucunda üretilen çıktı tüm düğümler tarafından kayıt edilerek sonucu bildirilir. Akıllı sözleşmeler tarafından gerçekleştirilen her transfer işlemi ağda bulunan tüm düğümler tarafından defterlerine eklenerek kayıt edilir.

Blokzincir üzerinde yapılan herhangi bir işlem değiştirilemezdir ve birden fazla düğüm üzerinde bütünlüğüne zarar verilmeden yürütülebilmelidir. Bu nedenle, akıllı sözleşmelerin işlevini dağıtık olarak bir ağ üzerinde gerçekleştirebilmeleri için bazı özellikleri sağlamaları gerekmektedir.

Deterministiklik Bir akıllı sözleşme verilen aynı girdi ile her çalıştırıldığında aynı çıktıyı üretebilmelidir. Akıllı sözleşmelerin çıktıları blokzincire kayıt edilerek diğer düğümler tarafından tekrar işletilerek kontrol edilmesinden dolayı, bir düğümün kullandığı girdiler ile hesapladığı sonuç diğer düğümler tarafından da aynı sonuca ulaşılabilecek şekilde hesaplanabilmelidir.

Sonlandırabilirlik Hesaplama teorisinde sonlandırma problemi, bir programın tüm girdiler için sonlandırabilir olduğunu belirlenmesi problemidir. Alan Turing tarafından 1936'da bir Turing makinası programının sonlandırabilir olup olmadığını belirleyen bir algoritmanın var olamayacağını ispatlamıştır[78]. Ancak, bir akıllı sözleşme dağıtık olarak tüm düğümler üzerinde çalışması gerektiği ve sonucunun blokzincirde yayınlanması gerektiğinden dolayı sonlandırabilir olması gerekmektedir. Bir akıllı sözleşmenin sonlandırabilirliği test edilememesi nedeniyle bazı önlemler alınması gerekmektedir. Bunlardan ilki, programın atlama işlemi yapabilmesi engellenerek turing eksikliği sağlanması yolu ile sonsuz döngüye girmesi engellenerek gerçekleştirilebilir. Ancak bu durum programın işlevselliğini sınırlamaktadır. Diğer bir önlem ise bir sayaç ile işlemlerin sayılarak hesaplanmasıdır. Program işletilirken yapılan her adım önceden belirlenmiş adım miktarına denk gelmektedir. Program için ayrılmış olan adım sayısı bittiğinde program sona ermemiş ise sonlandırılabilmektedir. Ethereum blokzincirinde bahsedilen sayaç, gaz ücreti ödenerek ile işlem miktarı sınırlandırılmaktadır.

Gaz, Ethereum'da kullanılan özel bir birimin adıdır. Akıllı sözleşmelerde çalıştırılan programın sonlandırıldığından emin olunabilmesini sağlamasının yanı sıra bir eylemin veya bir eylemler dizisinin gerçekleştirmesi için ne kadar işlem yapılması gerektiğini belirten bir ölçü birimidir. Akıllı sözleşmede harcanan gaz miktarının işlem ücretine dönüştürülebilmesi için gaz ücreti sözleşmeyi oluşturan kişi tarafından belirlenir. Eğer gaz ücreti çok düşük belirlenmiş ise madenciler işlem başına daha yüksek ücret elde edebilecekleri sözleşmeleri işletmeyi tercih edebilirler. İşlem ücretleri gaz üzerinden hesaplanmakla beraber, ödeme Ether cinsinden yapılmaktadır.

Yalıtılmışlık Açık izinsiz bir blokzincire herkes tarafından akıllı sözleşme programları yüklenebilmektedir. Eğer sözleşmeler yalıtılmamış ise, bilinen ve bilinmeyen hatalar veya zararlılar tarafından sistem bütün olarak etkilenebilme potansiyeline sahiptir.

Tablo 3.1: Blokzincir türleri

	İzinsiz	**İzinli**
Açık	Herkes verileri okuyabilir. Herkes transferleri işleyerek defteri güncelleyebilir.	Herkes transfer işlemlerini okuyabilir. Ancak sadece öntanımlı düğümler transferleri işleyerek defteri güncelleyebilir.
Özel	Sadece öntanımlı düğümler transfer işlemlerini görüntüleyebilir. Tüm öntanımlı düğümler transfer işlemlerini işleyerek defteri güncelleyebilir.	Sadece öntanımlı düğümler transfer işlemlerini görüntüleyebilir. Ancak öntanımlı düğümlerden sadece yetkileri olanlar transfer işlemlerini işleyerek defteri güncelleyebilir.

Bu nedenle, sözleşmelerin yalıtılmış bir ortamda yürütülmesi kritiktir. Ethereum blokzincirinde sözleşmeler, olabilecek negatif etkilerden sakınmak amacıyla Ethereum Sanal Makinası (Ethereum Virtual Machine, EVM) içerisinde çalıştırılmaktadır.

3.3 Blokzincir Tipleri

Blokzincir ağları, veri erişimine göre Tablo 3.1'de belirtildiği üzere iki farklı şekilde sınıflandırılabilmektedir. Bunlardan ilki verinin okunabilirliğine göre ayrılan açık/özel blokzincirlerdir. Açık bir blokzincir ağına herhangi biri istediği zamanda dahil olup ayrılabilmektedir. Açık blokzincir üzerinde kayıtlı olan veri herkes tarafından bir erişim yetkisine tabi tutulmaksızın okunabilir. Özel blokzincirlerde ise veriye erişim sadece öntanımlı olarak yetkili düğümler tarafından yapılabilmektedir.

Blokzincire veri yazma hakkına göre izinli/izinsiz blokzincir olmak üzere ikiye ayrılır. İzinli blokzincir türünde sadece izin verilen düğümlerin defteri güncelleme hakkı bulunmaktadır. Bu anlamda sadece belirlenmiş düğümler tarafından blok oluşturulabilmektedir. Özel izinli blokzincir ağlarında sadece izin verilen düğümler ağa erişebilirken, blok oluşturarak defteri güncelleme sadece yetkili düğümler tarafından yapılabilmektedir.

3.4 Kriptografik Yapıtaşları

3.4.1 Şifreleme

Analiz edilen e-seçim sistemlerinde kullanılan başlıca şifreleme algoritmaları burada özet olarak açıklanmaktadır.

3.4.1.1 ElGamal Şifreleme

ElGamal şifreleme sistemi[79], Diffie-Hellman anahtar paylaşımına[80] dayanan bir asimetrik açık anahtar şifreleme yöntemidir. Taher ElGamal tarafından 1985 yılında keşfedilmiştir. ElGamal şifrelemenin güvenliği ayrık logaritma problemine dayanmaktadır. ElGamal şifreleme anahtar üretimi, şifreleme ve şifre çözme olmak üzere üç prosedürden oluşur.

Anahtar Üretimi Mertebesi q olan döngüsel grup G ve üreteci g olmak üzere,

1. $x \in 1, ..., q-1$ olmak üzere rastgele bir x sayısı seçilir.
2. $h = g^x$ hesaplanır.
3. Açık anahtar (G, q, g, h) olmak üzere şifreleme yapılması için yayınlanır. x değeri şifre çözme amacıyla kullanılacak olan gizli anahtardır.

Şifreleme Bir açık anahtar (G, q, g, h) kullanılarak m mesajını şifrelemek için aşağıdaki adımlar takip edilir.

1. $y \in 1, ..., q-1$ olmak üzere rastgele bir y sayısı seçilir.
2. $c_1 = g^y$ hesaplanır.
3. $s = h^y$ hesaplanır. s paylaşılan sırdır.
4. $c_2 = m \cdot s$ hesaplanır.
5. Şifreli metin (c_1, c_2) olarak atanır.

Şifre Çözme Şifreli metin (c_1, c_2)'nin şifresini x gizli anahtarı ile çözmek için aşağıdaki adımlar takip edilir.

1. $s = c_1^x$ olacak şekilde paylaşılan sır hesaplanır.
2. $m = c_2 \cdot s^{-1}$ olarak hesaplanır.

Homomorfik Özellikler ElGamal şifreleme çarpma işlemi üzerine homomorfik özelliklere sahiptir.

Şifreli metinlerin çarpılması Aynı anahtar ile şifrelenmiş şifreli metinlerin çarpımı, açık metinlerin çarpımına eşittir.

$$\begin{aligned} E_{pk}(m_1) \cdot E_{pk}(m_2) &= (c_1^{y_1}, m_1 \cdot h^{y_1}) \cdot (c_2^{y_2}, m_2 \cdot h^{y_2}) \\ &= (c_1^{y_1+y_2}, m_1 \cdot m_2 \cdot h^{y_1+y_2}) \\ &= E_{pk}(m_1 \cdot m_2) \end{aligned}$$

3.4.1.2 Paillier Şifreleme

Paillier şifreleme, 1999 yılında Pascal Paillier tarafından ortaya atılmış olasılıksal açık anahtarlı şifreleme algoritmasıdır. n'inci kök sınıfları hesaplama zorluğuna dayanır. Ayrıca toplama üzerine homomorfik özelliklere sahiptir.

Paillier şifreleme anahtar üretimi, şifreleme ve şifre çözme prosedürlerinden oluşmaktadır.

Anahtar Üretimi

1. İki büyük asal sayı p ve q, $obeb(pq, (p-1), (q-1)) = 1$ eşitliğini sağlayacak şekilde seçilir. Bu p ve q değerlerinin eşit uzunlukta olduğunu garanti eder.
2. $n = pq$ ve $\lambda = EKOK(p-1, q-1)$ olarak hesaplanır.
3. $g \in \mathbb{Z}_{n^2}^*$ olmak üzere rastgele bir g sayısı seçilir.

4. L fonksiyonu $L(u) = \frac{u-1}{n}$ şeklinde tanımlanmak üzere $\mu = (L(g^\lambda \mod n^2))^{-1}$
5. $(n, g) \leftarrow$ Açık anahtar (Şifreleme)
   $(\lambda, \mu) \leftarrow$ Gizli anahtar (Şifre çözme)

Alternatif olarak eşit uzunlukta p ve q kullanılırsa, anahtar üretimi aşağıda belirtildiği gibi daha basit bir yöntem ile üretilebilir.

$$\varphi(n) = (p-1)(q-1) \mod n$$
$$g = n + 1 \mod n$$
$$\lambda = \varphi(n) \mod n$$
$$\mu = \varphi(n)^{-1} \mod n$$

Şifreleme $m \in \mathbb{Z}_n$ olmak üzere m şifrelenecek bir mesaj olsun.

1. $r \in \mathbb{Z}_n^*$ olacak şekilde rastgele bir r değeri seçilsin. $EBOB(n, r) = 1$ olduğundan emin olun.
2. Şifrelenmiş metin c hesaplanır.

$$c = g^m \cdot r^n \mod n^2$$

Şifre Çözme $c \in \mathbb{Z}_{n^2}^*$ olmak üzere c bir şifreli metin olsun.

1. Mesaj $m = L(c^\lambda \mod n^2) \cdot \mu \mod n$ olarak hesaplanır.

Homomorfik Özellikler Homomorfik şifreleme, şifreli metinlerinin üstünde uygulanan işlemlerin açık metin üzerinde de etkisinin olmasıdır.

$$E(m_1) + E(m_2) = E(m_1 + m_2)$$

Paillier şifreleme toplama işlemi üzerine homomorfik özelliklere sahiptir.

Şifrelenmiş metinlerin toplanması Aynı anahtar ile şifrelenmiş iki kapalı metinin çarpımı, açık metinlerin toplamına eşittir.

$$\begin{aligned} E_{pk}(m_1) \cdot E_{pk}(m_2) &= (g^{m_1} r_1^n) \cdot (g^{m_2} r_2^n) \mod n^2 \\ &= g^{m_1+m_2}(r_1 r_2)^n \mod n^2 \\ &= E_{pk}(m_1 + m_2) \end{aligned}$$

Şifrelenmiş metin ile açık metinin toplamı Şifrelenmiş bir metin ile açık bir metinin çarpımı açık metinlerin toplamına eşittir.

$$\begin{aligned} E_{pk}(m_1) \cdot g^{m_2} &= (g^{m_1} r_1^n) \cdot g^{m_2} \mod n^2 \\ &= g^{m_1+m_2}(r_1)^n \mod n^2 \\ &= E_{pk}(m_1 + m_2) \end{aligned}$$

Şifrelenmiş metin ile açık metinin çarpımı Şifrelenmiş bir metin ile açık bir metinin çarpımı açık metinlerin toplamına eşittir.

$$\begin{aligned} E_{pk}(m_1)^{m_2} &= (g^{m_1} r_1^n)^{m_2} \mod n^2 \\ &= g^{m_1 \cdot m_2}(r_1^n)^{m_2} \mod n^2 \\ &= g^{m_1 \cdot m_2}(r_1^{m_2})^n \mod n^2 \\ &= E_{pk}(m_1 \cdot m_2) \end{aligned}$$

Not: $r \in \mathbb{Z}_n^*$ olduğunda $r^{n\lambda} \equiv 1 \mod n^2$ olmasıyla şifre çözümü sırasında etkisiz hale gelmesinden ötürü r değerlerinin farklı olması n inci kuvvete sahip olduğu sürece önemli değildir.

3.4.2 İmzalama

Analiz edilen e-seçim sistemlerinde kullanılan başlıca imzalama teknikleri burada özet olarak açıklanmaktadır.

3.4.2.1 RSA Kör İmzalama

Kör imzalama (blind signinig), 1983 yılında David Chaum[11] tarafından önerilmiştir. Mesajın içeriğinin imzalama işleminden önce gizlenerek, imza atan kişiye mesajı göstermeden imzalamasına olanak vermektedir. Protokolun sonunda imzayı atan kişi mesaj hakkında bir bilgi elde edememesine rağmen, orjinal mesaj üzerine atılmış imza geçerliliğini korumaktadır. RSA kör imzalama basit olarak gerçeklenebilen kör imzala algoritmalarından biridir.

1. Mesaj imzalayacak kişiye gönderilmeden önce köreltme işlemi uygulanır.

$$m' = m \cdot r^e \mod N$$

2. İmzalayan kişi gizlenmiş mesaj m''e normalde RSA'de imzaladığı gibi imza oluşturur.

$$s' \equiv sign(m') \equiv (m')^d \equiv m^d \cdot r^{ed} \mod N$$

3. $e\cdot \equiv 1 \mod N$ olmasından dolayı, imza s''nün üzerindeki gizleme faktörü r geri alınabilir.

$$\begin{aligned} s &= s' \cdot r^{-1} \mod N \\ &= m^d \mod N \end{aligned}$$

4. İmza değeri s, m mesajı için geçerli olur. RSA imza doğrulama prosedürü uygulanarak geçerliliği test edilebilir.

RSA kör imzalama tekniğinde imzayı atan kişi ne imzaladığını görmediği için, eğer aynı anahtar ile şifrelenmiş bir şifreli metin köreltilerek imzalatılırsa imzayı atan kişiye mesaj

deşifre ettirilebilir. Bu nedenle imzalama ve şifreleme anahtarlarının birbirinden bağımsız olarak ayrıca üretilmesi ve tek bir amaç için kullanılması gerekmektedir.

3.4.2.2 Halka İmzalama

Belirli bir grubun herhangi bir üyesi tarafından oluşturulabilen dijital imza türüdür. İmzanın grubun bir üyesi tarafından oluşturulduğu bilinmesine rağmen, hangi üyenin imzayı oluşturduğunu bulmak hesapsal olarak mümkün değildir. Ron Rivest, Adi Shamir ve Yael Tauman tarafıdnan 2001 yılında önerilmiştir, [81].

İmza oluşturma Grup üyelerin açık anahtarları $(P_1, P_2, \ldots, P_n)$ olmak üzere, x_s gizli anahtarı ile m mesajı için halka imza σ oluşturma adımları aşağıda belirtildiği gibidir.

1. E_k için kullanılacak simetrik anahtar $k = H(m)$ olarak hesaplanır.
2. Rastgele olacak şekilde bir υ değeri seçilir.
3. İmzayı oluşturan hariç grubun her üyesi için rastgele olacak şekilde bir x_i değeri belirlenerek, $y_i = g_i(x_i)$ değeri bulunur.
4. y_s için halka denklemi çözülür.
5. İmzayı oluşturanın özel anahtarı ile $x_s = g_s^{-1}(y_s)$ olacak biçimde hesaplanır.
6. $(P_1, P_2, \ldots, P_n; \upsilon; x_1, x_2, \ldots, x_n)$ olarak imza oluşturulur.

Doğrulama Halka imzası σ ve grup üyelerin açık anahtarları $(P_1, P_2, \ldots, P_n)$ girdi olarak verildiğinde eğer imza geçerli ise doğru, değilse yanlış çıktısı verilir. İmza doğrulama işlemi 3 adımdan oluşur.

1. Açık anahtar trap door fonksiyonu tüm x_i'lere $y_i = g_i(x_i)$ olarak uygulanır.
2. Simetrik anahtar $k = H(m)$ olarak hesaplanır.
3. Halka denklemi $C_{k,\upsilon}(y_1, y_2, \ldots, y_n) = \upsilon$ olduğu test edilir.

3.4.3 Sıfır Bilgi İspatı

Sıfır bilgi ispatı, bir kişinin bir bilgiyi bildiğini başka bir kişiye bu bilgiye dair herhangi bir bilgi açıklamadan ispat edebilmesidir, [82]. Bir sıfır bilgi ispatı şu üç özelliği sağlamalıdır:

- Tamlık (Completeness): Eğer ifade doğru ise, dürüst bir doğrulayıcı, ispatlayanın bilgiye sahip olduğundan emin olabilmelidir.
- Doğruluk (Soundness): Eğer ifade yanlış ise, hile yapan bir ispatlayıcı dürüst bir doğrulayıcıyı hesapsal olarak ikna edememelidir.
- Sır vermemek (Zero knowledge): Eğer ifade doğru ise, doğrulayıcı ifadenin doğru olduğu dışında hiç bir bilgi elde edememelidir.

3.4.3.1 Schnorr Sıfır Bilgi İspatı

Ayrık logaritma $log_g y \mod n$ değerinin bilindiğini ispatlamak için kullanılır.

1. İspatlayan rastgele bir r değeri üreterek bunu doğrulayıcıya $t = g^r$ olarak taahhüt eder.
2. Doğrulayıcı rastgele bir sorgu değeri c seçerek ispatlayana gönderir.
3. İspatlayan c sorgusuna karşılık olarak $s = r + cx$ değerini hesaplayarak doğrulayana gönderir.
4. Doğrulayan $g^s = ty^c$ eşitliğinin sağlanıp sağlanmadığını kontrol eder.

Eğer eşitlik sağlanıyor ise, ispatlayan $log_g y$'e karşılık gelen x değerini biliyor demektir.

3.4.3.2 Fiat-Shamir Heuristic

Etkileşimli sıfır bilgi ispatı tabanlı dijital imza üretmek için kullanılan bir tekniktir. Böylece, gizli bir sayının bilindiği, gizli sayıya dair herhangi bir bilgi sızdırılmadan açık olarak ispatlanabilir. Yöntem Amos Fiat ve Adi Shamir tarafından 1986 yılında[83] önerilmiştir. Sabit rastgele üreteç iki tarafında bildiği veriler ile oluşturulabildiği sürece, etkileşimli bir sıfır bilgi ile kanıt protokolünü etkileşimsiz hale çevirmek için kullanılabilir.

Schnorr sıfır bilgi ispatının özet fonksiyonu kullanılarak etkileşimsiz hale dönüştürülmüş hali aşağıda belirtildiği gibidir.

1. İspatlayan rastgele bir r değeri üretir ve $t = g^r$ olarak r değerini taahhütünü oluşturur.
2. İspatlayıcı $c = H(g, y, t)$ olarak bir sorgu değeri hesaplar.
3. İspatlayan c sorgusuna karşılık olarak $s = r + cx$ değerini hesaplar.
4. İspat (r, s) olarak oluşturulmuş olunur.

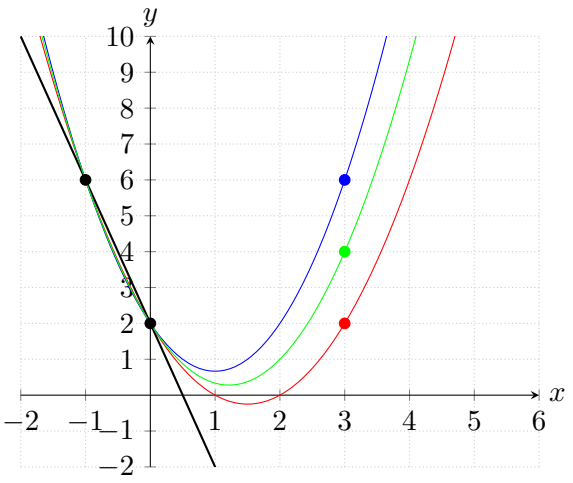
Doğrulayıcı, ispatlayan ile etkileşime girmesine gerek kalmaksızın $t \equiv g^r y^c$ eşitliğinin sağlanıp sağlanmadığını kontrol eder.

3.4.4 Shamir'in Gizli Paylaşım Algoritması

Gizli paylaşım[84], gizli bir bilginin bir grup katılımcıya her biri paylaştırılan sırrın bir parçasını alacak biçimde dağıtılmasıdır. Paylaştırılan gizli bilgi sadece yeterli sayıda paydaş bir araya gelerek tekrardan oluşturulabilmektedir. Paylaştırılmış parçalar tek başlarına gizli bilgiye dair bir anlam ifade etmezler.

Bir gizli paylaşım şemasında bir *dağıtıcı* ve n adet *katılımcı* bulunur. Dağıtıcı, katılımcılara sadece belirli bir koşul yerine getirildiğinde dağıtılan sırrın tekrardan oluşturulabileceği şekilde sırrı parçalara bölerek dağıtır. Bu koşul, katılımcılardan en az t adet kişiden oluşan bir grubunun sırrı yeniden yapılandırabileceği, ancak t adet kişiden daha az bir grubun oluşturamayacağı şekilde pay vererek gerçekleştirir. Bu yapıdaki bir sisteme *(t, n) eşik şeması* denilmektedir.

Shamir'in sır paylaşımı, Adi Shamir tarafından keşfedilmiş[84] bir sırrın parçalara bölünerek n adet katılımcıya dağıtıldığı ve en az t adet katılımcının bir araya gelerek sırrı tekrardan oluşturabileceği bir sır paylaşımı algoritmasıdır. Algoritmanın temeli, derecesi d olan herhangi bir polinomu en az $d+1$ noktanın tanımlayabilmesi gerçeğine dayanmaktadır. Şekil 3.4'de gösterildiği üzere, her bir polinom aynı iki nokta üzerinden geçmesine rağmen üçüncü bir nokta tarafından ifade edilebilmektedir.



Şekil 3.4: Her bir polinom aynı iki nokta üzerinden geçmesine rağmen üçüncü bir nokta tarafından ifade edilebildiğine dikkat ediniz.

Özellikler Shamir'in Gizli Paylaşımı, teorik olarak güvenli bir şifreleme sistemidir. Bu, sınırsız bir hesaplama gücüne sahip bir saldırganın sistemi kırmak için yeterli bilgiye sahip olmadığı anlamına gelir. Ayrıca, t eşiği sabit tutulduğu sürece, diğer parçalar etkilenmeden yeni katılımcılar dinamik olarak eklenebilir veya silinebilir.

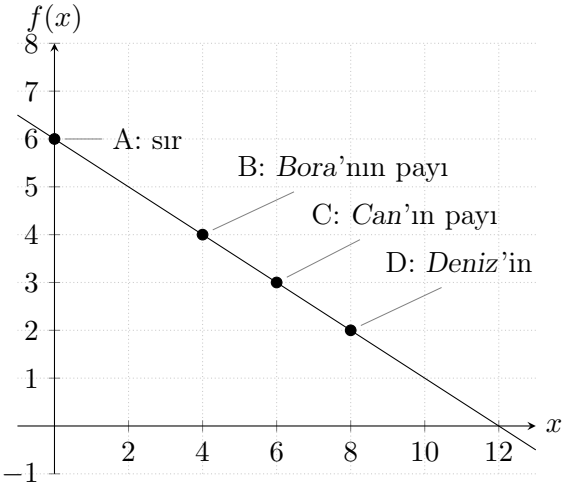
Hazırlık *Ayşe*'nin bir sırrı s, n adet parçaya şu kurallar ile ayırmak istediğini farz edelim:

- Herhangi bir $\leq d$ adet parça kombinasyonu sırrı öğrenemesin.
- Herhangi bir $> d$ adet parça kombinasyonu sırrı öğrenebilsin.

Ayşe derecesi d olan bir polinom f'i, $f(0) = s$ olacak şekilde üretir.

$$\begin{aligned} pay_1 &= (1, f(1)) \\ pay_2 &= (2, f(2)) \\ &\vdots \\ pay_n &= (n, f(n)) \end{aligned} \tag{3.1}$$

Ayşe her katılımcıya parçalardan farklı birini verir.



Şekil 3.5: Herhangi iki nokta çizginin formülünü ortaya çıkarabilir. $f(0)$'a karşılık gelen değer sırrın kendisidir.

Tekrar Oluşturma Sırrı ortaya çıkarmak için gizli polinom formülü elde edilmelidir. Eğer herhangi t adet nokta biliniyorsa, polinom formülü *Lagrange interpolasyon polinomu yöntemi* ile tekrardan oluşturulabilir. Örneğin, şekil 3.5'de gösterilen B, C veya D noktalarından en az ikisi bilinmesi durumunda sır A hesaplanabilmektedir.

$$P(x) = \sum_{j=1}^{n} y_j \prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{x - x_k}{x_j - x_k} \tag{3.2}$$

Bölüm 4

Blokzincir Tabanlı Bazı E-Seçim Sistemlerinin Analizleri

Bu bölümde, blokzincir tabanlı e-seçim önerilerinin sağladıklarını iddia ettikleri güvenlik meselelerini ele alınmaktadır. Analizleri gerçekleştirirken, kullanılan bilinen kriptografik algoritmaların güvenliği sağladığı varsayılarak, bu çalışmada ana odak e-seçim kriterlerinin yerine getirilip getirilmemesinin irdelenmesidir. Blokzincir ile ilgili problemler hali hazırda Heiberg ve arkadaşları tarafından yapılan çalışmada [85] detaylı olarak analiz edildiğinden, burada detaylara girilmemiştir.

4.1 E-voting System Based on the Bitcoin Protocol and Blind Signatures

Cruz vd. [21] tarafından önerilen sistem, Bitcoin [36] protokolüne ve kör imzalama [11] tekniklerine dayanmaktadır. Ayrıntılara girmeden sistem, blok zincirindeki şeffaflığı korurken seçmen ile oy pusulasının arasındaki bağı kırabilmek için ÖBK (Ön ödemeli Bitcoin Kartı) kullanımı ve kör imzalamadan faydalanmaktadır.

Sistemde rol almakta olan seçmen, yönetici ve sayım sorumlusu olmak üzere 3 aktör bulunmaktadır. Sistem adım adım belirtildiği üzere üç aşama olarak aşağıdaki gibi gösterilebilir.

4.1.1 Kayıt Aşaması

Öncelikle seçim prosedürlerinin başlatılabilmesi için yönetici boş pusula formatını yayınlar. Daha sonrasında, yönetici ve seçmen tarafından takip edilmesi gereken kayıt aşaması adımları aşağıda belirtildiği gibidir.

1. Her seçmen V_i, seçimde oy kullanabilmek için kimlikleri ve kendileri tarafından rastgele oluşturulmuş k anahtarıyla şifrelenmiş tercihleri ile beraber kayıt olurlar.

2. Seçmen tarafından tercihlerinin şifrelenmiş hali x_i köreltme fonksiyonundan geçirilerek x_i' değerini oluşturur. $x_i' = blind_e(x, r)$

3. Köreltilmiş mesaj x_i' yöneticiye imzalanması için gönderilir. Eğer seçmenin oy kullanmaya hakkı bulunuyorsa yönetici mesajı imzalar.

   Yöneticinin mesaj üzerindeki imzası seçmenin geçerli bir seçmen olduğunu belirtmektedir. Bu aşamada kullanılan kör imzalama tekniği, imzalatılmak istenen asıl değer x_i imzalayan kişiye ifşa edilmeden x_i üzerinde geçerli bir imza oluşturabilmesini sağlamaktadır.

4. Yönetici imza değeri $d_i = sign_A(x_i')$ ile birlikte her bir seçmene Bitcoin üzerinde işlem ücretini karşılamak amacı ile bir ÖBK verir. Sistemde seçmenin mahremiyeti, Bitcoin üzerinde iz sürülememesi için ÖBK'nin bir zarf içerisinde verilmesi ile sağlamaktadır.

Kayıt aşaması sonlandırıldıktan sonra yönetici tarafından köreltilmiş mesajları ile birlikte kimliklerini göndermiş olan ve bir imza talebinde bulunan geçerli seçmenler listesi L_{voters}, $< ID, x_i' >$ formatında yayınlanmaktadır.

4.1.2 Oy Kullanımı Aşaması

Seçmen oy kullanmak için aşağıda belirtilen adımları takip eder.

1. Seçmen kayıt sırasında aldığı ÖBK'den kendi bitcoin adresi $V_i.BA$'ya bir işlem gerçekleştirir.

   Her bir seçmen anonimliğini ve mahremiyetinin bozulmadığından emin olmak için verilen ÖBK'ındaki parayı kendileri tarafından oluşturulmuş adreslere aktarmalıdır. Yönetici tarafından verilmiş olan tüm ÖBK'larının açık adresleri yayınlandığında, ÖBK'nin kullanımının seçimin güvenliğini ve dayanıklılığını arttırdığı yazar tarafından belirtilmektedir.

2. Seçmen, oyunun kullanmak için $V_i.BA$'dan $A.BA$'a OP_RETURN içerisinde $< x_i, y_i >$ değerlerini barındıracak şekilde bir işlem oluşturur.

   Bu işlem, seçmenin oyunun taahhüdü ile birlikte oy kullanmaya uyguluğunu herkes tarafından doğrulanabilmesini sağlamaktadır.

Oy kullanım aşaması sona erdiğinde, yönetici işlemlerin ve OP_RETURN içeriklerinin imzalarını doğrulayarak $< V_i.BA, x_i, y_i >$ barındıracak şekilde sayım sırasında kullanılmak üzere bir geçerli pusula listesi $L_{ballots}$ yayınlar. Bu aşamanın sonunda, L_{voters} ve $L_{ballots}$ listeleri eşit sayıda elemana sahip olmalıdır.

4.1.3 Sayım Aşaması

Seçmenler ve sayım sorumlusu seçim sonucunu elde edebilmek için aşağıda belirtilen adımları takip ederler.

1. Seçmen, $V_i.BA$ adresinden sayım sorumlusunun $C.BA$ adresine OP_RETURN içeriğinde oyunu kayıt sırasında şifrelediği anahtar $< k_i >$'yi barındıracak şekilde bir işlem oluşturur.

2. Sayım sorumlusu $L_{ballots}$ listesinden blokzinciri de kontrol ederek seçmenin uygunluğunu kontrol eder.

3. Sayım sorumlusu x_i mesajını k_i anahtarını kullanarak şifresini çözer ve elde ettiği oy değerine göre adayın hanesine bir ekler.

Son olarak, sayım sorumlusu tüm mesajları deşifre ettikten sonra seçim sonucunu duyurur.

4.1.4 Gereksinim Analizi

Seçme Hakkı: Dürüst bir yönetici tarafından kullanılan imza algoritmasının güvenli olduğu varsayılırsa, yönetici dışında kimse geçerli bir imza y_i oluşturamaz. Sistemde seçme hakkının imzanın geçerliliğine dayanmasından dolayı, bu özellik sistem tarafından sağlanmaktadır.

Emsalsizlik: Emsalsizlik özelliği $< x_i, y_i >$ çiftinin eşsiz olmasına dayanmaktadır. Yazarların belirttiğine göre, $< ID_i, x_i' >$ listesinin kayıt aşamasında yayınlanmasından dolayı dürüst olmayan bir yönetici dahi aynı seçmen için birden fazla geçerli imzayı fark edilmeden oluşturamamaktadır. Bu sebeple bir seçmen sadece bir geçerli oy kullanabilmektedir. Emsalsizlik özelliği seçim sistemi tarafından sağlanmaktadır.

Bağışlayıcılık: Seçmen, seçimde kullanacağı oy tercihini kayıt aşamasında oluşturup yöneticiye imzalatmaktadır. Yönetici aynı seçmen için birden fazla imza oluşturması halinde sistemin tasarımından kaynaklı olarak emsalsizlik gereksinimine aykırı bir durum oluşmasından dolayı, seçmenin tercihini değiştirmesi mümkün değildir. Bu nedenle, bağışlayıcılık özelliği seçim sistemi tarafından sağlanamamaktadır.

Dayanıklılık: Yazarlar, eğer bir seçmen k anahtar değerini sayım sorumlusuna iletemeden Bitcoin adresinin özel anahtarını kaybederse, başka bir adresten k değerini gönderebileceklerini belirtmişlerdir. Bu durum, başka birinin seçmen adına doğru olmayan bir k anahtar değeri göndererek seçmenin oyunun iptal edilmesine neden olabilecek bir takım kusurların oluşmasına neden olabilir. Bu durumunun önüne geçebilmek adına bir

oy için birden fazla k değeri iletildiği durumlar için oy formatında bir doğrulama mekanizmasının olması gerekmektedir. Çünkü doğru anahtar sadece seçme hakkına sahip geçerli bir seçmende bulunmaktadır ve oy değeri değiştirilememektedir. Yayınlanan makalede açıkça belirtilmemesine rağmen anlaşıldığı kadarıyla oy pusulasında böyle bir doğrulamanın bulunduğunu varsayılmıştır. Seçimde rol alan kimsenin seçim gidişatını değiştirememesinden dolayı bu sistem dayanıklılık özelliğini sağlamaktadır.

Adillik: Yazarların makalelerinde belirttikleri üzere, bir seçmen kendi elinde bulundurduğu k anahtar değerini oy kullanma aşaması sona ermeden sayım sorumlusuna gönderebilmektedir. Bu durumda kullanılan oy değerleri herkese açık olarak paylaşılacağından ötürü seçim sonucu kısmi olarak hesaplanabilmektedir. Böyle bir problemin oluşmasından kaçınmak için yazarlar oy kullanma aşaması devam ettiği sürece sayım sorumlusunun açık adresinin gizli olarak tutulması gerektiğini önermişlerdir. Ancak, seçmenler ellerinde bulundurdukları k anahtar değerlerini diğer yollardan yayınlayarak, örneğin bu amaç ile oluşturulmuş bir websitesi üzerinden, kısmi sonuçlar elde edebilmeleri mümkündür. Bu durum adillik özelliğini ihlal etmektedir. Dolayısıyla, adillik özelliği sistem tarafından sağlanmamaktadır.

Mahremiyet: Seçmen mahremiyeti, kör imzalama teknikleri ile birlikte ÖBK ve seçmenin açık Bitcoin adresinin anonimliğine bağlıdır. Bitcoin üzerinde gerçekleştirilen transfer işlemlerinin kökenine kadar geri takip edilebilmesinden dolayı[86], yukarıda bahsedilen adreslere bağlı herhangi bir adresi ifşa edilmiş dikkatsiz bir seçmenin oyu ile kimliği arasında bağ kurabilmesine olanak tanımaktadır. Yazarlar bu durumu yukarıda bahsi geçen adreslerin sadece ve sadece seçimde oy kullanmak amacı ile kullanılması gerektiğini belirtmişlerdir. Bu durumun yanı sıra, seçmen ÖBK'nın açık yada gizli adreslerinin kimliğini ifşa edecek şekilde kayıt altına alınmadığından emin olmalıdır. Bu durumdan yazarlar ÖBK'nin bir zarf içerisinde iletilmesi gerektiğini belirterek bahsetmişlerdir. Yine de, zarflar rastgele bir şekilde seçilmediği veya seçilmeden önce karıştırılmadığı durumlarda zarf içerisinde iletilmiş olsa bile bu problem devam etme potansiyeli göstermektedir. Dolayısıyla, mahremiyet seçmenin davranışına göre değişebildiği için sistem tam anlamı ile bir mahremiyet sağlamamaktadır. Ayrıca oyların açık olarak gönderilmesinden dolayı, devlet çapında (state-level) atak ile mahremiyet tehlike altındadır.

Baskı direncliliği: Bir seçmen üzerinde baskı kurmak isteyen bir saldırgan, seçmene kayıt sırasında oluşturması gereken gizli anahtar değeri k'yi ya da bu anahtar ile oluşturulan tercihi kendisi oluşturarak fark edilmeden seçmeni bu değerlerden birini kullanmak üzere zorlayabilmektedir. Saldırganın blokzincir üzerinde yayınlanan değerleri karşılaştırarak seçmenin davranışını tespit edebilmesinden dolayı, sistem baskı dirençliliği özelliğini sağlamamaktadır.

Makbuzsuzluk: Seçmenin tercihi sayım aşamasında anonim olarak pusulanın şifrelendiği anahtarın yayınlanması ile açıklanmaktadır. Burada anonimliği sağlamakta olan etmen kayıt sırasında oluşturulan pusulanın gönderildiğini Bitcoin adresinin normal şartlar altında seçmen kimliği ile bağının kurulamamasıdır. Bir seçmen, ÖBK'nin gizli anahtar değeri, oyunu göndermek için kullanmış olduğu Bitcoin adresinin özel anahtar değerini yada oyunu şifrelediği anahtar değeri k'yi kullandığı oyu ispatlamak amacı ile bir makbuz oluşturmak için kullanabilmektedir. Dolayısıyla, makbuzsuzluk özelliği seçim sistemi tarafından sağlanamamaktadır.

Bireysel Doğrulanabilirlik:

- Sunulan pusula formatının doğruluğu. Seçim süresince kullanılacak pusulalar ve barındırdığı değerler seçimin başlangıcında yönetici tarafından yayınlanmaktadır. Dolayısıyla seçmenin kendisine iletilen pusulanın formatını yayınlanmış olan listeden kontrol edebilmesinden dolayı, bu kontrol sistem tarafından sağlanmaktadır.

- Kullanıldığı gibi kayıt:

  Bitcoin kripto parasının altyapı olarak kullandığı blokzincirin açık ve izinsiz bir blokzincir altyapısına sahip olmasından dolayı, bir seçmen kullanmış olduğu oyun ve anahtar değerinin kaydının doğru olarak yapılıp yapılmadığının kontrolünü bloklara eklenen transfer işlemlerini takip ederek yapabilmektedir. Bunun yanı sıra, seçmen yönetici tarafından yayınlanan doğrulanmış listeleri blokzincirdeki değerleri ile karşılaştırarak oylarını doğrulayabilmektedir. Dolayısıyla, bu kontrol sistem tarafından sağlanmaktadır.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu: Seçmenler tarafından seçimde kullanılmış olan şifrelenmiş oy pusulaları, karşılığı olan anahtar değerleri açıklanana kadar kontrol edilememektedir. Anahtar değerler yayınlandıktan sonra, herhangi biri şifreli oy pusulasının şifresini çözerek yayınlanmış olan aday listesinden bir değer içerip içermediğini inceleyebilmektedir. Eğer herhangi bir pusula geçersiz oy tercihi barındırmakta ise, herhangi biri bu durumu kullanılan blokzincirin açık ve izinsiz olmasından dolayı tespit edebilecektir. Bunun yanı sıra, yayınlanmış listeden değerler kullanılarak fazla oy yada negatif oy oluşturmanın mümkün olan bir yolu yoktur. Dolayısıyla seçim sistemi kullanılmış oyların formatının doğruluğu kontrolü sağlamaktadır.

- Kayıt edildiği gibi sayım: Bitcoin'in açık ve izinsiz bir blokzincir altyapısına sahip olmasından dolayı, seçim verileri açık olarak erişilebilirdir. Herhangi biri, sayım sorumlusu tarafından açıklanan sonucun doğruluğunu, geçerli oyları kendisi de sayarak doğrulayabilmektedir. Bu nedenle sistem kayıt edildiği gibi sayım kontrolünü yerine getirmektedir.

- Tutarlılık: Herhangi biri yayınlanmış olan kullanılmış oylar listesi ile sayılan oylar listesini karşılaştırarak seçimin tutarlılığını doğrulayabilmektedir. Yazarlar tarafından belirtildiği üzere, listelerin birbiri ile tutarsız olması durumu sadece dürüst olayan bir yönetici tarafından oluşturulabilirdir. Bu durumun açık olarak sayım aşamasında tespit edilebilmesinden dolayı, sistem tutarlılık kontrolünü sağlamaktadır.

- Kayıt edilen her oy "kullanıldığı gibi kayıt" kontrolüne tabi tutulur: Seçmenlerin kimlikleri ile birlikte seçimde kullandıkları oy pusulalarının şifrelenmiş biçimlerinin kayıt aşamasında yayınlanmasından dolayı, dürüst olmayan bir yönetici oy kullanmamış olan seçmenler adına fark edilmeden oy oluşturamaz.

4.2 Internet Voting Using Zcash

Tarasov vd. [52] tarafından önerilen seçim sistemi, Zcash[51] kripto parasının altyapısını herhangi bir şekilde değiştirmeden sistemin mahremiyet özelliklerinden faydalanmaktadır. Sistem, her bir seçmenin geçerli bir kimliğinin seçimde oy kullanabilmesi için yasal haklarının kontrol edilebileceğini varsayım olarak kabul etmektedir.

Sistem, birbirini takip eden 4 ayrı aşamadan oluşmaktadır. Bu aşamalar sırası ile kayıt, davet, oy kullanımı ve sayım aşamalarıdır.

4.2.1 Kayıt Aşaması

Kayıt aşaması, sistemde bir seçmenin oy kullanabilmek için takip etmesi gereken ilk aşamadır. Seçmenin, kimlik doğrulamasının gerçekleştirildiği adımdır. Ayrıca, seçmenlerin oy kullanıp kullanmadığının takip edilebilmesi için gereklidir.

Bu adımlar aşağıda belirtildiği gibidir.

1. Seçmen kayıt sayfasına gider.
2. Seçim sistemi seçmene kimliğini doğrulamak amacıyla bir bilmece gönderir.
3. Seçmenin istemcisi, kimlik bilgilerini kullanarak bilmeceyi çözer ve elde ettiği sonucu sisteme geri iletir.
4. Seçim sistemi, eğer bilmeceye karşılık gelen çözüm doğru ise seçmenin sertifikasını seçim veritabanına kayıt eder.

Başarılı bir kayıt işleminin ardından, organizatör seçmenin e-posta adresini bir sonraki adımda kullanmak üzere kayıt altına almıştır.

4.2.2 Davet Aşaması

Davet aşaması, seçim sisteminin kayıt olmuş olan her bir seçmen için atanmış tek kullanımlık eşsiz bir bağlantıyı e-posta yoluyla ilettiği aşamadır.

1. Seçim organizatörü, seçim bilgilerini sisteme girer.

2. Seçim sistemi yeni bir seçim oluşturduktan sonra, kayıtlı olan her bir seçmene kendilerine atanmış olan eşsiz bağlantıyı gönderir.

Başarılı bir davet aşaması sona erdiğinde tüm seçme hakkına sahip kayıtlı seçmenler eşsiz bir bağlantıyı elde etmiş olmalıdır.

4.2.3 Oy Kullanımı Aşaması

1. Seçmen, Zcash cüzdanında bir adet t-adresi oluşturur. Bu adres, adaylara gönderilecek olan bir adet ZEC jetonunun teslim edildiğinden emin olmak için oluşturulmaktadır.

2. Seçmen kendisine gönderilen bağlantıyı takip ederek bir önceki adımda oluşturduğu t-adresi ibraz eder.

3. Sistem sunucusu eğer seçmen daha önce ZEC talep etmediyse seçmenin ibraz ettiği adrese bir adet ZEC gönderir. Bununla birlikte, sistem seçmenin durumunu veritabanında günceller ve teslim edilmiş ZEC miktarını belirten sayacı bir arttırır.

4. Seçmen Zcash cüzdanında bir adet z-adres oluşturur. T-adresi üzerinden teslim almış olduğu ZEC'i oluşturduğu z-adresine aktararır.

5. Seçmen z-adresine aktardığı miktarı bu adres üzerinden tercihi olan adayın adresine göndermek için Zcash üzerinde bir işlem oluşturur.

Bu aşamada adayın alıcı adresinin tipine göre değişiklik gösteren iki adet sistem varyantı bulunmaktadır.

- Adayın z-adres kullandığı varyant:

  Zcash kripto parasında z-adresler arası işlemler daha önceki bağlantıları kırmakta olduğundan dolayı, adaylar cüzdanlarında teslim almış oldukları oy miktarlarını seçim havuzuna geri teslim ettiklerinde, seçmenler kullandığı oyların seçim sonucu hesaplanırken sayıldığını doğrulayamayacaktır. Bu varyant seçmene daha iyi bir mahremiyet ortamı sağlarken, seçmenin sisteme daha çok güvenmesini gerektirmektedir.

- Adayın t-adres kullandığı varyant:

  Adaylara gönderilmiş olan oy miktarları herhangi biri tarafından gerçek zamanlı olarak takip edilebilecektir. Ayrıca gönderilen miktarların geçmiş işlemlerle olan bağlantıları korunabileceğinden ötürü, seçmenler kullanmış oldukları oyun sayılıp sayılmadığını takip edebileceklerdir.

Kullanılan varyant ne olursa olsun, gönderilen oyların seçmenin z-adresinden gönderilmesinden dolayı yapılan JoinSplit aktarım işlemi blokzincirde doğrulanabilir bir şekilde kayıt altına alınmaktadır.

4.2.4 Sayım Aşaması

Seçimin son aşaması kullanılan oyların sayımı ve denetimidir.

1. Adaylar kendilerine gönderilen tüm ZEC miktarlarını t-adresleri üzerinden ZEC havuzunun t-adresine gönderirler.

Sayım aşamasının sonunda, sistem tarafından seçmenlere verilmiş olan toplam ZEC miktarı ile adayların havuza gönderdikleri ZEC miktarı eşit olmalıdır.

4.2.5 Gereksinim Analizi

Seçme Hakkı Seçmenler, seçimin başında kimlikleri ile birlikte kayıt olmaktadırlar. Eğer seçmen oy kullanmak için uygun özelliklere sahipse, seçim sistemi seçmene bir ZEC iletmektedir. Bir diğer taraftan, oy jetonunun tam olarak 1 ZEC değerine karşılık gelmesinden ötürü, 1 ZEC'e sahip olan herhangi biri adayın adresine korumalı işlem oluşturarak para transferi gerçekleştirebilir. Sistemde bu oy kullanmaya karşılık gelmektedir. Sistemin veritabanından seçmenin daha önce oy kullanıp kullanmadığını kontrol etmesine rağmen, korumalı işlemlerin detaylarını inceleyemeyeceği için, dürüst olmayan bir katılımcı cüzdan üzerinden işlemi gerçekleştirebilir. Bu nedenle yürütülen seçimde oy hakkı bulunmayan birisi oy kullanabilmektedir. Bu durum seçim hakkı özelliğini ihlal etmektedir.

Emsalsizlik: Emsalsizlik seçmene teslim edilen ZEC miktarı ile ilişkilidir. Seçme hakkı özelliğinde bahsedilmiş olan saldırı durumu, burası için de geçerlidir. Yöneticiler kendi t-adreslerinden seçmenin t-adresine açık bir şekilde görüntülenebilen bir işlem yapmış olsalar dahi, ZEC'in seçim sistemi dışından tedarik edilebilmekte olmasından dolayı, bir seçmen cüzdanından transfer işlemi gerçekleştirerek birden fazla oy kullanabilmektedir. Bu durum her seçmenin en fazla bir geçerli oy kullanabilmesini gerektiren eşsizlik özelliğini ihlal etmektedir.

Bağışlayıcılık: Zcash kripto para sistemi, bir para sisteminin gerekliliği olarak aynı paranın birden fazla defa kullanılmasına müsade etmemektedir. Sistemde oy kullanım prosedürünün aslında para transferi işlemi olarak kurgulanmasından dolayı dürüst bir seçmenin kendilerine iletilen ZEC jetonunu sadece bir defa gönderebilme şansı bulunmaktadır. Sistemin, seçmenlere kullandıkları oyları değiştirme imkanını sağlayacak başka bir yöntem sunmamasından dolayı bağışlayıcılık özelliği sistem tarafından sağlanamamaktadır.

Dayanıklılık: Yazarlar, adaylar için z-adres kullanıldığı sistem varyantında seçimi kaybettiğini anlayan adayın oy kullanım aşaması bittikten sonra seçmenlerden almış olduğu tüm ZEC miktarını havuza geri dönmeyebileceğini belirtmişlerdir. Sistem bütünlüğünün toplamda gönderilen ZEC miktarı sayacı ile sağlanmasından dolayı bu durum seçimin güvenilirliğine gölge düşürmektedir. Ayrıca adayların adreslerindeki toplam miktarın gözlemlenememesinden dolayı hangi adayın dürüst olarak davranıp davranmadığını belirlemek mümkün değildir. Yazarlar bir sayaç daha ekleyerek adaya yapılan her transferin sayılabileceğini belirtmişlerdir, ancak bu korumalı transferler ile gerçekleştirilen işlemlerde açık olarak gözlemlenebilir biçimde uygulanabilir bir çözüm değildir.

Bu durumların yanı sıra, oy jetonlarının teslimi istemci tarafında çalıştırılan kod betiklerine dayandırılmıştır. Bir seçmenin sistemden ZEC talep ettikten sonra adaya göndermesi bu kod betiklerine dayandığından dolayı, iletilen jetonun adaya gönderildiği garanti altına alınamamaktadır.

Adillik: Adayların adreslerinin t-adres olarak belirlendiği varyantta, bu adreslere yapılan transfer işlemlerinin herkes tarafından açık bir şekilde erişilebilir olmasından dolayı seçim sonucu anlık olarak hesaplanabilmektedir. Adayların z-adres türünde adresler ile

oy topladıkları varyantta ise, sadece adaylar kendi almış oldukları oy miktarını biliyor olacaklardır. Oy kullanım süresi sona ermeden hiç kimsenin, adaylar dahil, kısmi yada erken sonuçları elde edememesi gerekmesinden dolayı her iki durumda da adillik gereksinimi sağlanamamaktadır.

Mahremiyet: Seçmen mahremiyeti, Zcash JoinSplit operasyonunun işlemlerin geçmişi ile bağları kırmasına dayanmaktadır. Bu bağ açık olarak kurulamayacağından dolayı ve Bitcoin kripto parasının aksine yapılan transfer işleminin tarihçesi ile bağının kırılmasından dolayı seçmen mahremiyeti sistem tarafından sağlanmaktadır.

Baskı dirençliliği: Seçmen tarafından beyan edilmesi gereken t-adresin sahipliği sistem tarafından doğrulanamayacağı için, bir saldırgan hedef aldığı seçmene kendi oluşturmuş olduğu adresi beyan etmeye zorlayabilir. Böyle bir durumda saldırganın sistem tarafından oy kullanımı için ZEC alıp almadığını tespit edebilmesinden dolayı, seçmenin tarif edildiği gibi davranıp davranmadığı saldırgan tarafından ayırt edilebilmektedir. Bu durumda seçmenin saldırganın tarif ettiği durum dışında saldırganı aldatabileceği bir yöntem bulunmamaktadır. Bunun yanı sıra yazarlar, saldırgan tarafından seçmenlerin e-posta adreslerine seçmenden önce erişim elde edebildiği durumlarda seçmenden önce e-posta ile gönderilen linki kullanarak seçmenin adına kendi tercihlerini oy olarak kullanma girişiminde bulunabileceğini belirtmişlerdir. Bahsedilen durumlara sistem tarafından bir hafifletmeye ya da önleme yapılamaması nedeniyle bu seçim sistemi baskıya dayanıklılık göstermemektedir.

Makbuzsuzluk: Zcash kullanıcı dokümantasyonunda [87] belirtildiği üzere, kullanıcılar korumalı adresleri için muhasebe ve denetim amacıyla, üçüncü partilerin görüntüleme erişimi verebilmek için bir görüntüleme anahtarı (viewing key) oluşturabilmelerine olanak sağlamaktadır. Zcash kripto para sisteminin sağlamış olduğu bu özellik, bir seçim sistemi için seçmenin kullanmış olduğu oyun makbuzunu oluşturabilmesi anlamına gelmektedir. Kullanmış olduğu oyu ispatlamak isteyen yada zorunda bırakılan bir seçmenin görüntüleme anahtarını API sayesinde elde edebilmesinden dolayı, seçim sistemi makbuzsuzluk özelliğini sağlayamamaktadır.

Bireysel Doğrulanabilirlik:

- Sunulan oy pusulası formatının doğruluğu: Oy pusulaları seçmenlere sistem tarafından bir link aracılığıyla gönderilmektedir. Gönderilen pusulaların bütünlüğünün korunduğunun açık bir şekilde seçmen tarafından doğrulanabilir olması gerekir. Seçim sisteminde böyle bir özellikten bahsedilmemiştir. Seçmenler kendilerine gönderilen oy pusulalarında bulunan adayların adreslerini doğrulayamadıklarından ötürü, sistem bu kontrolü sağlayamamaktadır.

- Kullanıldığı gibi kayıt: Seçmen, oyunu kullanmak için oluşturuduğu işlemi blokzincir üzerinde doğrulayarak oyunun doğru olarak kayıt edilip edilmediğini kontrol edebilmektedir. Dolayısıyla sistem bu kontrolü sağlamaktadır.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu: Eğer adayların adresleri t-adres olarak belirlenmişse, bu adreslere gönderilmiş olan miktarlar herhangi biri tarafından açık olarak kontrol edilebilmektedir. Diğer taraftan, eğer adaylar z-adres kullanmakta ise, adayların her bir oy ile aldıkları miktar görüntülenememektedir. Negatif miktar gönderimi Zcash protokolünde yasaklanmış olsa dahi, fazla oy kullanımı durumunda herhangi biri bu durumu tespit edemeyecektir.

- Kayıt edildiği gibi sayılma: Eğer adayların adresleri t-adres olarak belirlenmişse, herhangi biri adaylara gönderilen miktarları blokzincir üzerinden erişip toplayarak adayın almış olduğu oy miktarını seçim sonucu ile karşılaştırarak doğrulayabilmektedir. Öte yandan, eğer aday adresleri için z-adres kullanılmışsa, adayların almış olduğu oy miktarlarına adayların kendileri dışındaki kişilerce erişmek mümkün olmayacaktır. Her iki varyant göz önüne alındığında, kimse gönderilmiş oyların geçerli bir seçmen tarafından gönderilip gönderilmediğini doğrulayamamaktadır.

- Tutarlılık: Sistem, ekstra oyların bulunmadığından bir sistem sayacı kullanarak göndermiş olduğu ZEC miktarını adayların toplamış olduğu ZEC miktarları ile karşılaştırarak sağlamaktadır. Ancak seçmenlerin bir kısmının dürüst olmadığı bir durumda, örneğin sistemden ZEC talebinde bulunup gönderilmiş olan miktarları oy kullanma amacı ile kullanmadıkları durumlarda, ekstra oy kullanılmış ise bu sayaçlar ile fark edilemeyecektir. Bir diğer mesele ise, seçimi kaybettiğini anlayan

adayların ellerinde bulunan tüm miktarı havuza geri dönmemesidir. Bu durumda seçimin bütünlüğünün sağlandığı doğrulanamayacaktır. Bu nedenlerle, sistemde herhangi biri tarafından bir tutarsızlık olduğunda bu durum tespit edilemeyeceğinden dolayı sistem tutarlılık kontrolünü sağlamamaktadır.

- Kayıt edilen her oy "kullanıldığı gibi kayıt" kontrolüne tabi tutulur: Zcash protokolünde korumalı hesaplardan işlem yapıldığında işlem tarihçesi arasındaki bağ koparılması nedeniyle, bir oyun uygun bir seçmen tarafından gönderilip gönderilmediğinin açık bir şekilde herkes tarafından kontrolü yapılamamaktadır.

Yazarların bahsettiği diğer meselelerden biri olan ihlal edilmiş oy makinalarıdır. Bu sistemde oy makinaları kullanıcıların cihazlarıdır. Baskı kurmaya çalışan bir saldırganın tüm seçim sistemini ifşa etmek yerine, kullanıcıların cihazları ifşa etmesinin çok daha kolay olduğunu belirtmişlerdir. Bahsi geçen bir diğer mesele ise, dürüst olmayan seçmenlerin kendilerine gönderilmiş olan ZEC miktarını cüzdanlarına geldiği sırada çalmaya çalışmalarıdır. Burada yapılan varsayım, bir betiğin cüzdana gelen spesifik bir işlemi algılayıp, gelen miktarı seçmenin tercih etmiş olduğu adayın hesabına yönlendirmesidir. Bu durumun önüne geçmek için en ufak para birimi olan 1 zatoshi kullanımı önerilmiştir. Eğer oy için kullanılan miktar küçük olursa teşebbüsler de azalacaktır. Ancak yinede bu durum seçimin tutarlığının sağlanamamasına engel olmamaktadır. Tüm bunların yanı sıra, Zcash'in güvenilir bir kurulum gerektiriyor olması, bir seçim sisteminin altyapısı olarak kullanılmaya uygun olup olmadığına yönelik ayrıca bir tartışma konusudur.

4.3 An E-voting System Based on Blockchain and Ring Signatures

Yifan Wu vd. [53] tarafından önerilen seçim sistemi Bitcoin [36] ile yüzük (ring) imzalama algoritmalarından [81] faydalanmaktadır. Sistemde 3 farklı rolde aktör bulunmaktadır. Bunlar seçmenler (V_i), Kayıt otoritesi (RA) ve Seçim otoritesidir (EA).

Sistem kullanılan özet algoritmasının ($sha256$) güvenli olduğunu, kayıt otoritesi ile seçim otoritesinin çakışmadığını ve sistemdeki tüm aktörlerin seçim sürecine kaydını yaptırmak için gerekli adımları takip ettiğini varsaymaktadır.

Sistem 3 temel aşamadan oluştumaktadır. Bunlar sırası ile hazırlık ve kayıt aşaması, oy kullanım aşaması ve sonuç aşamasıdır.

4.3.1 Hazırlık ve Kayıt Aşaması

Hazırlık ve kayıt aşaması seçmenlerin ve adayların seçim sistemine kayıt yaptırdığı süreçler ile birlikte seçim otoritesinin tüm seçmenlerin açık anahtarlarını ring imzası oluşturabilmek için topladığı aşamadır.

Hazırlık safhası: Bir seçimin başlatılabilmesi için seçim otoritesi aşağıda belirtilen adımları takip eder.

1. Seçim otoritesi kendi özel anahtarı SK_b'yi sisteme kayıt eder.
2. Sistem kayıt edilen özel anahtar SK_b ile Bitcoin adresi A_{EA}'yi üretir.
3. Seçim otoritesi seçim ID'si (L_i), seçim ismi, toplam seçmen sayısı n ve açıklamayı sisteme girer.
4. Seçim sistemi $A_1, A_2, ..., A_n$ olacak şekilde Bitcoin adreslerini adres havuzu olarak üretir.

Aday kayıt safhası:

1. Seçimde aday olmak için, kişi kimliği ile birlikte kayıt otoritesine yüz yüze başvurur.
2. Kayıt otoritesi, eğer adayın kimliği doğrulanabiliyorsa adayın gereken bilgilerini sisteme kayıt eder. Bununla birlikte adaya aday ID'si C_i'yi teslim eder.

Seçmen kayıt safhası:

1. Seçmen, kayıt olmak için kimliği ile birlikte kayıt otoritesine yüz yüze başvurur.
2. Kayıt otoritesi, eğer seçmenin oy kullanma hakkı varsa e-posta adresini sisteme kayıt eder. Kayıt otoritesi rastgele oluşturulmuş kayıt bağlantısı LK_i'yi adayın e-posta adresine gönderir.
3. Seçmen ring imzalamada kullanacağı açık anahtar çifti (SK_i, PK_i)'yi oluşturur.
4. Seçmen oluşturmuş olduğu açık anahtar PK_i'yi kendisine gönderilen bağlantıyı takip ederek ibraz eder. Özel anahtarı SK_i'yi gizli kalacak şekilde saklar.

Seçmen kayıt safhası sonunda, seçimde oy kullanacak tüm adaylar listesi sabit bir n sayısı olmalıdır. Bu nedenle seçmen kayıt safhası sona erdikten sonra kayıt otoritesi yeni seçmen kaydı yapamaz.

Anahtar yayınlama safhası Kayıt aşaması sona erdikten sonra, seçim otoritesi oylamayı başlatmak için aşağıda belirtilen adımları takip eder.

1. Kayıt olmuş oy kullanma hakkı bulunan tüm adayların açık anahtarları ring imzasında kullanılmak üzere seçim otoritesi tarafından yayınlanır.
2. Seçim otoritesi kendi Bitcoin adresinde k adet BTC üretir.
3. Seçim otoritesi adres havuzundaki her bir A_i adresine k/n kadar BTC'yi işlem ücretini karşılaması için gönderir.

4.3.2 Oy Kullanımı Aşaması

1. Seçmen aday listesinden tercih ettiği adayın ID'si C_i'yi seçim ID'si L_i ile birlikte seçer.

2. Kayıt otoritesi tüm seçmenlerin açık anahtar kümesi $(PK_1, ..., PK_n)$'yi seçmene gönderir.

3. Seçmen tercih ettiği adayın ID'si C_i'i imzalamak için kayıt sırasında ürettiği özel anahtar SK_i, kayıt otoritesinden aldığı açık anahtar değerleri $PK_1, ..., PK_n$'i kullanarak σ imza değerini hesaplar. Sistem $(\sigma, sha256(\sigma))$ çiftini ayrıca kayıt altına alır.

4. Seçmen yayınlanmış olan Bitcoin adres havuzundan rastgele seçtiği bir adres A_i'nin özel anahtarı SK_{A_i}'yi teslim almak için seçim otoritesini başvurur. Seçim otoritesi eğer seçmen tarafından daha önce bir anahtar talebinde bulunulmamışsa anahtarı seçmene teslim eder.

5. Seçmen, seçim otoritesinden özel anahtarını teslim aldığı adresi kullanarak A_{EA} Bitcoin adresine OP_RETURN içerisinde c_i değerini barındıracak şekilde bir işlem oluşturarak gönderir.

$$c_i = encode(sha256(\sigma(C_i, SK_i, (PK_1, ..., PK_n))), C_i, L_i)$$

4.3.3 Sayım Aşaması

Eğer aynı A_i adresinden birden fazla işlem oluşturulmuşsa, sistem ilk gönderilen değeri sayıp daha sonrasında gönderilenleri görmezden gelecektir.

1. Seçim sistemi, kayıt altına aldığı tüm $(\sigma, sha256(\sigma))$ çiftleri ve tüm açık anahtar listesi PK ile yanıtlayacaktır.

2. Seçim sistemi, seçim otoritesinin Bitcoin adresine yapılan tüm Bitcoin ödemelerinin OP_RETURN içeriğinin kodlarını çözerek $sha256(\sigma)$ değerinden σ ve C_i değerlerini oluşturacaktır.

3. Seçim sistemi tüm imzaların doğrulamasını kontrol edecektir. Her geçerli doğrulama yapıldığında ilgili adayın hanesine 1 ekleyecektir.

4.3.4 Gereksinim Analizi

Seçme Hakkı: Bir seçmenin oy kullanabilmesi için ring imzası oluşturabiliyor olması gerekir. Ring imzası ancak kayıt işlemi sırasında oy kullanma hakkı bulunan kimliği doğrulanmış seçmenlerden toplanan açık anahtarlardan en az birinin gizli anahtar değeri biliniyorsa oluşturulabilir. Listede bulunmayan bir seçmen adayı yayınlanan açık anahtar kümesinden en az birinin gizli anahtar değerini bulması uygulanabilir olmadığından dolayı imza oluşturamayacaktır. Sistem seçme hakkı özelliğini sağlamaktadır.

Eşsizlik: Bir seçmenin sahip olduğu aynı gizli anahtar ile birden fazla ring imzasını farklı adayların ID'lerini imzalamak için kullanmasına engel olacak bir kısıtlama yoktur. Oyunu kullanmak için bir sonraki adım, seçim otoritesine oluşturmuş olduğu ring imzası ile birlikte tercihini bir Bitcoin işleminde `OP_RETURN` alanı içerisinde göndermesi gerekmektedir. Protokolde belirtildiği üzere seçim sonucu sadece Bitcoin adres havuzundan gerçekleştirilen işlem için yapılmaktadır. Seçim otoritesi aynı seçmen için havuzdan birden fazla adresi iletmemesinden dolayı seçmen ikinci bir işlem gerçekleştirmiş olsa dahi kendisine gizli anahtarı teslim edilmiş BTC adresinden transferi yapılmalıdır. Yazarların belirttiklerine göre aynı adresten yapılan ekstra işlemlerin göz ardı edilmesinden dolayı bir seçmen bir seçimde en fazla bir geçerli oy kullanabilmektedir.

Bağışlayıcılık: Emsalsizlik gerekliliğinin analizinde bahsedildiği üzere yazarlar sayım aşamasında ring imzalarının geçerliliği ile birlikte gönderilen ilk doğrulanabilir oyun geçerli olarak sayıldığını belirtmişlerdir. Geçerli ilk oyun sayılmasından dolayı bir seçmenin seçim süresi boyunca kullanmış olduğu oyu değiştirebilmesi için sunulan herhangi bir yöntem bulunmamaktadır. Sistem bağışlayıcılık özelliğini karşılamamaktadır.

Dayanıklılık: Seçmenler tarafından oluşturulan ring imzaların tüm hali sistem veritabanında kayıt altına alınmaktadır. Blokzincir üzerindeki özet değerlerinden imza değerlerine ulaşılamayacağı için sistem veritabanının ifşa olduğu yada bir arıza nedeni ile veri kaybı yaşandığı bir durumda oluşturulan seçim sonucu doğrulanamayabilir. Dolayısıyla dayanıklılık gereksinimi sistem tarafından karşılanmamaktadır.

Adillik: Yazarların belirttiğine göre, seçim sonuçları oy pusulaları açık metin olarak herhangi biri tarafından tüm seçim süreci boyunca erişilebilmesinden dolayı seçim sonuçları gerçek zamanlı olarak hesaplanabilmektedir. Sistem bu gereksinimi karşılayamadığını belirtmiştir.

Mahremiyet: Yazarlar transfer işlemine dahil edilen OP_RETURN içerisine kayıt edilen değerlerin herhangi biri tarafından çözülebileceğini belirtmişlerdir. Seçmenin, seçim otoritesinden havuzda bulunan seçmiş olduğu bir adresin özel anahtarını temin etmesinden dolayı ve bu aşamada sistemin seçmenin kimliğini doğrulaması gerekmesinden dolayı, seçim otoritesi oyun kullanıldığı adres ile seçmen arasında bağ kurabilme potansiteline sahiptir. Ayrıca ilk ve son oyu kullanan seçmenlerin kimlikleri ile kullandıkları oyların arasında bağ kurulabilme olasılığı oldukça yüksektir. Sistem mahremiyet gereksinimini karşılamamaktadır.

Baskı Dirençliliği: Blokzincire kayıt edilen imzaların özetinden, sistem API'si sayesinde imzalar herhangi biri tarafından elde edilebilmektedir. Ancak, ring imzalarının özelliği olarak, imzayı atan kişinin kimliği imzalama sırasında kullandığı açık anahtar miktarı kadardır. Yazarlar, bu durumda baskı direncinin ancak seçmen sayısı yüksek olduğunda sağlanabileceğini belirtmişlerdir. Bir diğer yandan, seçmenlerin kayıt safhasından sonra anahtarlarını kendileri oluşturmaları beklenmesi sebebi ile, bir saldırgan seçmeni kendi oluşturmuş olduğu anahtarı kullanmaya zorlayabilir. Ayrıca, bu durum blokzincir üzerinde saldırgan tarafından takip edilebilmektedir. Saldırganın özel anahtarı bildiği benzer bir durumda saldırgan grubu tanımlayabilir, [88]. Böyle bir durumda seçmenin özel anahtarı ile birlikte açık anahtarını da değiştirebilmesi gerekir. Ancak ring imzalarının doğası nedeni ile tüm imzaların değiştirilmesine neden olacağından dolayı uygulanabilir değildir. Baskı altında oyunu kullanmak durumunda kalmış bir seçmenin kullanmış olduğu oyu değiştirememesi nedeni ile sistem baskı dirençliliği özelliği göstermemektedir.

Makbuzsuzluk: Yazarlar, seçmenin oy kullanma aşamasında ring imzası oluşturduktan sonra bir işlem ID'si elde ettiklerini belirtmişlerdir. Seçmenin bu işlem numarasını oyunu ispatlamak için kullanmaya çalıştığı bir durumda, blokzincirden herhangi bir işlem ID'sini söyleyebileceğinden dolayı seçmenin dürüst davranıp davranmadığı anlaşılamaz.

Ancak oyların açık olarak kayıt edilmesinden dolayı, oy gönderme transfer işlemi yapılan Bitcoin adresinin özel anahtarının bilindiğinin ispatlanması ile bir makbuz oluşturulabilmektedir. Bu nedenden dolayı sistem makbuzsuzluk özelliğini sağlamamaktadır.

Bireysel doğrulanabilirlik:

- Sunulan pusula formatının doğruluğu: Aday numaraları seçmenlere açık bir API aracılığıyla verilmesine rağmen, protokolde aday numaraların bütünlüğünün doğrulanabileceği bir metottan bahsedilmemiştir. Sistem bir seçmene diğer seçmenlere gönderdiğinden farklı bir pusula formatı ile çelişen bir pusula gönderebilir. Böyle bir durumda seçmen pusulanın doğruluğunu kontrol edemeyecektir. Bu durumda API üzerinden gönderilen aday bilgilerinin kontrolü sağlanabilmelidir.
- Kullanıldığı gibi kayıt: Ring imzalarının özet değerleri ile birlikte tercih değeri blokzincir üzerinde kayıtlı tutulması nedeniyle sisteme kayıt edilen değerlerin değiştirilip değiştirilmediği, API tarafından sağlanan imzaların elde eldilebilmesinden dolayı seçmen tarafından, tercihinin doğru olarak kayıt edilip edilmediği kontrol edilebilmektedir. Ring imzasını herhangi bir seçmen oluşturabilmesine rağmen Bitcoin adresleri üzerinde yapılan işlemler adresin gizli anahtar değeri ile oluşturulan imza sayesinde bütünlüğünün korunmasından dolayı imza, başka bir seçmenin madenci olduğu durumlarda da korunmaktadır.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu: Kullanılan oyların değerlerinin açık olarak kayıt edilmesinden dolayı herhangi biri değeri inceleyebilmektedir ve formatı yanlış olan bir oy tespit edilebilecektir. Bunun yanı sıra sistemde oy tercihleri çoktan seçmeli ve açık olması nedeniyle negatif ya da fazla oy kullanmanın mümkün bir yolu yoktur.
- Kayıt edildiği gibi sayılma: Kayıt edilen oy değerinin imza özetinin blokzincire kayıt edilmesinden ve imzaların açık olarak sağlanmasından dolayı bir seçmen kullanmış olduğu oyunun sayılıp sayılmadığını seçim sonucunu hesaplayarak doğrulayabilir. Oy tercihinin de imza özeti ile birlikte blokzincire yazılmasından dolayı, ring imzası tekrardan oluşturulsa bile tercih değiştirilemeyecektir. Ancak sistem veritabanının

ifşa olduğu bir durumda seçmenin imzası silinirse yada değiştirilirse blokzincirdeki değerler ile uyuşmayacağından ötürü seçmenin oyu iptal edilebilir. Böyle bir durumda, herhangi biri tarafından bir seçmenin oyunun geçersiz olması, blokzincire taahhüdü kayıt edilmesinden dolayı tespit edilebilecektir.

- Tutarlılık: Daha önce bahsedildiği üzere herhangi biri kayıt edilen oylar ile birlikte sayılan oyları karşılaştırabilmektedir. Blokzincirde kayıt edilen oylar ile sistem veritabanında kayıt edilen oyların tamamının herkesin erişimine açık olmasından dolayı, herhangi biri iki listeyi karşılaştırabilmektedir. Blokzincir üzeirndeki verinin değiştirilememesinden dolayı, eğer sistem veritabanı ifşa edilmişse bu durum açık olarak tespit edilebilecektir.

- Kayıt edilen her oy "kullanıldığı gibi kayıt" işlemine tabi tutulur:

  Geçerli bir oy pusulası oluşturabilmek için bir seçmen blokzincir üzerinde bir işlem oluşturarak imza özetini kayıt altına alırken, sistem veritabanına da imza değerlerini kayıt ettirmektedirler. Seçim otoritesinin yüzük imzasında kullanılan açık anahtarlardan en az birinin gizli anahtarını bildiği durumda, Bitcoin adres havuzundaki kullanılmamış tüm adreslerin özel anahtarını bilmesinden dolayı oyunu kullanmamış bir seçmen yerine oy kullanabilmektedir. Böyle bir durumda oyunu kullanmamış olan seçmen dahil kimse başkasının adına oy kullanıldığını tespit edemeyecektir.

Tüm bunların yanı sıra, seçmen sayısının fazla olduğu geniş ölçekli bir seçimde yüzük imzalama algoritmalarının kullanılması performans problemlerini önemli derecede öne çıkarmaktadır. Bitcoin blokzincir kripto parası dağıtık bir altyapıya sahip olmasına rağmen, sistem veritabanı kullanılmasından dolayı tek arıza noktası olarak gösterilebilir. Bir diğer mesele ise, günümüzde Bitcoin parasının maddi değerinin yüksek olması, seçim maliyetini önemli derece olumsuz olarak etkilemektedir.

4.4 An E-Voting Protocol Based on Blockchain

Yi Liu vd. [54] tarafından önerilen sistem blokzincir [36] ve kör imzalama [11] algoritmalarına dayanmaktadır. Önerilen sistem diğerlerinden farklı olarak geniş ağa ve kullanıcıya sahip güvenilen blokzincirler yerine elektronik seçim amacı ile tasarlanan ayrı bir blokzincir altyapısı kullanmaktadır. Protokol güvenilir üçüncü partinin sorumluluğunu birden çok varlığa dağıtmaktadır. Protokolde tanımlanan 3 ayrı rolde aktör bulunmaktadır. Bunlar seçmenler, organizatörler ve gözlemcilerdir. Tüm katılımcılar blokzincir üzerinde adresleme ve işlem oluşturma amacı ile kendilerine ait bir asimetrik anahtar çiftine sahiptir. Bunun yanı sıra organizatörler ve gözlemciler oy değerlerini imzalamak için ayrıca bir anahtar çiftine sahipken, her bir seçmen anonim olarak işlem oluşturma amacı ile kendi oluşturduğu bir anahtar çiftine sahiptir.

4.4.1 Kayıt Aşaması

1. Seçmen blokzincir üzerinde işlem yapmak için iki çift asimetrik anahtar çifti $(pk_{voter_i}, sk_{voter_i})$ ve (pk'_i, sk'_i) oluşturur.

2. Seçmen kimlik bilgilerini açık anahtarı pk_{voter_i} ile bir işlem oluşturarak organizatöre göndermek amacıyla işlem oluşturur.

3. Organizatör, seçmen bilgilerini doğrularsa seçmenin açık anahtarını uygun aday listesine ekler.

Kayıt aşaması bittiğinde organizatör tarafından seçimde oy kullanma hakkı bulunan adayları belirtmek için bir liste yayınlar.

4.4.2 Oy Kullanımı Aşaması

1. Seçmen aday tercihi ile birlikte aşağıdaki gibi belirtilen formatta bir oy dizisi V oluşturur.

$$V = \overbrace{\underbrace{01}_{\text{tercih}}\ \underbrace{000.....000}_{\text{y-bit sıfır dizisi}}\ \underbrace{10101001....000101010}_{\text{z-bit sözde rastgele dizi}}}^{\text{n bit oy dizisi}}$$

2. Seçmen, oluşturduğu oy dizisi V'nin özet değerini hesaplar. Oluşturduğu özet değerine $c' = blind(hash(V))$ olacak şekilde köreltme faktörünü uygular.

3. Seçmen kendi adresi pk_{voter_i}'den organizatörün adresi $pk_{organizer}$'e olacak biçimde c' değeri ile birlikte bir işlem oluşturur.

4. Organizatör kendine gönderilen mesaj c değerini eğer seçmenin açık adresi oy kullanmaya uygunluğu bulunan seçmen listesinde belirtilmiş ise ve henüz oy kullanmamışsa imzalayarak seçmenin adresine geri göndermek için bir işlem oluşturur. Eğer şartlardan biri sağlanmıyorsa mesajı görmezden gelir.

5. Seçmen organizatörle gerçekleştirdiği adımları her bir gözlemci için tekrarlar. Gözlemciler, organizatörler aynı prosedürlere uyarlar.

6. Seçmen, uyguladığı köreltme faktörünü organizatöre ve gözlemcilere imzalatmış olduğu mesajlardan çıkarır.

7. Seçmen, V değerini barındıran oy pusulası ile oyunu kullanmak için gizli olarak tuttuğu pk' adresinden organizatörün adresi $pk_{organizer}$ adresine V, $signature_{organizer}(hash(V))$, $signature_{inspector_j}(hash(V))$ değerlerini barındıracak biçimde gönderir.

4.4.3 Seçim Sonucu Aşaması

1. Organizatör blokzincir üzerinde gönderilmiş olan tüm pusulaları toplar ve üzerindeki imzaların doğrulamasını yapar.

2. Organizatör aşağıdaki listede belirtilen kriterler sağlanıyor ise pusulayı geçerli oylar kümesine ekler.

    - Pusula formatı geçerlidir.
    - Pusula zamanında gönderilmiştir.
    - Pusula üzerindeki tüm imzalar eksiksiz ve doğrulanabilirdir.
    - Pusula daha önce sayılmamıştır.

Seçim sonuçları, organizatör tarafından yayınlanan geçerli oylar kümesi ile birlikte duyurulur.

4.4.4 Gereksinim Analizi

Seçme Hakkı: Bir seçmenin uygunluğunu belirten anahtar komponent oy pusulasının özeti üzerindeki organizatörün ve gözlemcilerin imzalarıdır. Yazarlar, eğer organizatör ve gözlemciler birlikte gizlice anlaşmış ise suistimal durumunun oluşabileceğini belirtmişlerdir. Dürüst olmayan davranışları bastırmak amacıyla organizatör ve gözlemcilerin sayıların arttırılması önerilmiştir. Bu çözümün dezavantajı, blokzincir üzerinde daha fazla sayıda işlem yapılmasıdır. Bununla birlikte tüm işlemlerin blokzincir üzerinden gerçekleşmesi nedeniyle organizatör ya da gözlemcilerden biri görevini suistimal etmeye kalkarsa, herkes tarafında bu durum gözlemlenebilecektir.

Emsalsizlik: Seçmenin oyunu eşsiz kılan değer pusulanın parçalarından olan rastgele bit dizisi ve tercih değeridir. Protokolde bahsedildiği üzere aynı rastgele bit dizisine sahip olan oylardan sadece biri geçerli sayılmaktadır. Haliyle bir seçmenin birden fazla oy kullanabilmesi için pusulasının içeriğindeki rastgele değeri değiştirebilmesi gerekmektedir. Bu değişiklik organizatör ve gözlemcilerin imzalarını bozacağından dolayı pusulasını tekrardan imzalatması gerekmektedir. Organizatör ve gözlemcilerin daha önce bir seçmen için imza verdiği durumlarda aynı seçmen ID'si için kendilerine gelen mesajları göz ardı etmelerinden dolayı seçmen tekrardan pusula oluşturamayacaktır. Emsalsizlik gereksinimi sistem tarafından karşılanmaktadır.

Bağışlayıcılık: Emsalsizlik gereksinimi analizinde belirtildiği üzere seçmen tekrardan oluşturduğu pusula için gerekli imzaları elde edemeyecektir. Bu nedenle, geçerli sayılacak yeni bir oy pusulası oluşturması mümkün değildir. Oy tercihinin değiştirilebilmesi için başka bir yöntem sunulmamış olmasından dolayı bağışlayıcılık özelliği bulunmamaktadır.

Dayanıklılık: Organizatör ve ya gözlemcilerin imzalama görevlerini suistimal etmeleri halinde bu durum blokzincir üzerinde izlenebilir durumdadır. Ek olarak, seçmenlerin seçim prosedürü üzerinde olumsuz sonuçlar doğurabilecek bir yetkisi olmamasından dolayı dayanıklılık özelliği sağlanmaktadır.

Adillik: Oy pusulalarının açık izinsiz blokzincir altyapısı ile kayıt altına alınmasından dolayı açıkca görülebildiği gibi seçim sonuçları gerçek zamanlı olarak herhangi biri

tarafından kayıtlı oyların toplanması ile elde edilebilmektedir. Yazarlar bu problemi belirtmekte ve iki farklı öneri sunmaktadırlar. Bu önerilerden ilki izinli blokzincir kullanılmasıdır. Bu çözüm, belirttikleri üzere, seçim verisinin şeffaflığının azalmasına neden olacaktır. Diğer öneri ise organizatör tarafından sağlanan açık anahtar şifrelemesi anahtarı ile oyların şifrelenerek gönderilmesidir. Ancak bu durumda organizatörün seçim sonuçlarına oy verme süreci bitmeden erişmesi hala mümkün olmaktadır. Bir diğer mesele ise organizatörün seçim sonunda oyların şifesini çözecek anahtarı açıklamaması durumunda hiç kimsenin seçim sonucuna ulaşamayacak olması nedeniyle hali hazırda sağlanmakta olan dayanıklılık gereksinimi bozulacaktır.

Mahremiyet: Seçmen mahremiyeti özet fonksiyonun güvenliğine, kör imzalama prosedürüne ve blokzincir ağına dayanmaktadır. Yazarlar, blokzincir ağından kaynaklanan seçmenin IP adresinin ağ analizi ile ortaya çıkarılabileceğini ve seçmenin kullanmış olduğu oy ile kimliği arasında bağlantı kurulabileceğini belirtmişlerdir. Yazarların önerisi seçmenlerin Tor ağı gibi bir anonimlik servisi kullanmasıdır. Protokolde seçmen mahremiyeti oyların açıktan gönderilmesi nedeni ile ek bir servise ihtiyaç duyulmaksızın sağlanamamaktadır.

Baskı Dirençliliği: Saldırgan, seçmenden oluşturduğu anonim anahtar çiftini ifşa etmeye veya kendisi tarafından oluşturulmuş bir anahtar çifti kullanmaya zorlayabilmektedir. Bu durumda saldırgan blokzincir üzerinde açık anahtardan transfer işlemi yapılıp yapılmadığını takip ederek, seçmen davranışını tespit edebilmektedir. Bu durum baskı dirençliliği gereksinimini ihlal etmektedir.

Bir uzaktan seçim sisteminin baskı direncine sahip olabilmesi için seçmenlerin kullandıkları oyları oylama süreci boyunca değiştirebiliyor olması gerekmektedir [3]. Baskı altında oyunu kullanmak durumunda kalan bir seçmenin seçim süreci içerisinde oyunu değiştirememesi nedeniyle sistem baskı dirençliliği gereksinimini sağlayamamaktadır.

Makbuzsuzluk: Seçmenler anonim olarak blokzincirde işlem yapmak amacıyla oluşturduğu anahtar çiftinin özel anahtarı ile gönderilen oyun kendileri tarafından oluşturulduğunu ispatlayabilirler. Oyların açık olarak blokzincire kayıt edilmesinden dolayı, seçmen kullanmış olduğu oyu ispatlayabilmektedir. Bu durum makbuzsuzluk özelliğini ihlal etmesinden dolayı, özellik sistem tarafından sağlanmamaktadır.

Bireysel Doğrulanabilirlik:

- Sunulan pusula formatının doğruluğu: Sistemde adayların bilgilerinin nasıl yayınlandığından bahsedilmemektedir.
- Kullanıldığı gibi kayıt: Seçmenler blokzincir üzerinde oluşturdukları adresin gizli anahtarları ile işlemi imzalamalarından dolayı sadece kendileri tarafından oluşturabilecekleri işlemi kontrol ederek oylarının doğru kaydedilip kaydedilmediğini kontrol edebilmektedirler.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu:

  Oy pusulalarının blokzincir üzerinde açık metin olarak kaydedilmesinden dolayı herhangi biri tarafından formatın doğruluğu kontrol edilebilmektedir. Bunun yanı sıra kabul edilen çoktan seçmeli oy formatına göre negatif oy yada fazla oy kullanımı mümkün değildir. Kullanılan oyların formatının doğruluğu herhangi biri tarafından doğrulanabilmesinden dolayı sistem bu kontrolü sağlamaktadır.
- Kayıt edildiği gibi sayılma: Seçim sonuçlarının hesaplanması organizatörün blokzincir üzerinden pusulaları elde edip bir geçerli oy listesi yayınlaması ile yapılmasından ve blokzincire kayıt edilen verilerin değiştirilememesinden dolayı herhangi biri seçim sonucunu yayınlanan liste ile karşılaştırarak yayınlanan listenin geçerliliğini kontrol edebilir.
- Tutarlılık: Herhangi biri kayıt edilen oylar ile sayılan oylar listesini karşılaştırabilmektedir. Bu nedenle, listelerin farklı olduğu durum herhangi biri tarafından tespit edilebilecektir. Tutarlılık kontrolü sistem tarafından sağlanmaktadır.
- Kayıt edilen her oy "kullanıldığı gibi kayıt" kontrolüne tabi tutulur:

  Her bir seçmenin eşsiz bir oy pusulası oluşturmasından dolayı aynı oy pusulasının farklı seçmenlere ait olduğu bir durum ile karşılaşılması halinde herhangi biri bu durumu seçim verisini blokzincir üzerinde olmasından dolayı tespit edebilmelidir.

4.5 A Smart Contract for Boardroom Voting With Maximum Voter Privacy

Open Vote Network, McCory vd. [55] tarafından küçük ölçekli ve baskının az olduğu seçimlerde kullanılmak üzere maksimum seçmen mahremiyeti için tasarlanmış dağıtık iki adımlı bir seçim protokolüdür. Protokolün kendiliğinden sonuçları hesaplayabilme özelliğinden dolayı bir sayım otoritesine ihtiyaç duyulmamaktadır. Seçimde oy kullanmış herkes sayımı seçmen mahremiyetini ihlal etmeden yapabilmektedir. Ethereum blokzinciri üzerinde akıllı sözleşme olarak tasarlanmıştır. Bu nedenle, seçmenler protokolün doğru olarak yürütüldüğüne blokzincir üzerindeki mutabakata ile güvenebilmektedirler.

Günümüzde yaygın olarak kullanılan blokzincir gerçekleştirmelerinin veri kayıt ve transfer işlemi sayısı kısıtlamalarından dolayı, ulusal bir seçimde kullanılamayacağını, bu nedenle sunulan protokolün yönetim kurulu toplantıları gibi küçük çaplı seçimler için tasarlandığını belirtmişlerdir. Tüm seçmenlerin güvenli haberleşme kanalının bulunduğu varsayılmıştır. Ayrıca yazarlar yayınlarında seçimi sadece evet/hayır olacak biçimde ele almışlar ve çoklu seçenek için protokolün güvenlik ispatı [89] ile sunularak genişletilebileceğini belirtmişlerdir.

4.5.1 Kayıt Aşaması

Seçim yöneticisi uygun seçmen listesini $(V_1, V_2, ..., V_n)$ olarak yayınlar. Yönetici uygun olan her seçmenin hesap bilgisini oylama sözleşmesinde bulunan beyaz listeye ekler. Yayınlanan listede bulunan seçmenlerin kayıt aşamasında oylama anahtarlarını kayıt ettirmeleri gerekmektedir. Kayıt aşaması başlamadan önce seçmenler G üzerinde anlaşırlar.

1. Oy verme hakkı bulunan seçmen V_i, $x_i \in_R \mathbb{Z}_q$ olacak biçimde rastgele bir x_i gizli oylama anahtar değeri belirler.

2. Seçmen V_i, oylama anahtar değerini g^{x_i} olacak biçimde x_i değerini bildiğine dair sıfır bilgi ispatı $ZKP(x_i)$ ile birlikte yayınlar. Sıfır bilgi ispatı Fiat-Shamir heuristic [83] ile etkileşimsiz hale getirilmiş Schnorr ispatı [90] olarak gerçeklenmiştir.

Anahtar kayıt aşaması sonunda, her seçmen diğer seçmenler tarafından yayınlanmış olan ispatların geçerliliğini doğruladıktan sonra tekrardan oluşturulan anahtar değerleri Y_i listesini hesaplarlar.

$$g^{y_i} = Y_i = \prod_{j=1}^{i-1} g^{x_j} / \prod_{j=i+1}^{n} g^{x_j}$$

Yukarıda belirtilen formülde her seçmen V_i, diğer seçmenler tarafında yayınlanan değerleri g^{x_j} ile tüm seçmenler için g^{y_i} değerini hesaplayabilmektedir. $\sum_i x_i y_i = 0$ olmasından dolayı her bir seçmen $\prod_i g^{x_i y_i} = 1$ ifadesini oluşturabilmektedir.

4.5.2 Oy Kullanımı Aşaması

1. Seçmen tercihi v_i'yi $g^{x_i y_i} g^{v_i}$ olacak biçimde $v_i \in 0, 1)$ olduğunu etkileşimsiz sıfır bilgi ispatı ile birlikte yayınlar.

4.5.3 Seçim Sonucu Aşaması

Seçim sonucu oy kullanmış bulunan tüm seçmenler tarafından hesaplanabilmektedir. Bu nedenle bir sayım otoritesine ihtiyaç duyulmamaktadır. Tüm yayınlanan sıfır bilgi ispatları, oyların doğru formatta olduğunun kontrolü amacı ile doğrulanır. Bu aşamada tüm seçmenlerin oylarını kullanmış olmaları gerekmektedir.

1. Seçmen, $\prod_i g^{x_i y_i} g^{v_i}$ hesaplayarak seçim sonucunu $g^{\sum_i v_i}$ olarak bulunur.

Seçmen sayısının az olduğu kabul edilmesi nedeni ile, v_i değeri nispeten küçük bir değer olacağından tam kapsamlı arama ile bulunabilmektedir.

4.5.4 Gereksinim Analizi

Seçme Hakkı: Yönetici tarafından kontrol edilen bir sözleşmenin içerisine seçmen listesinin beyaz liste olarak eklenmesinden dolayı, seçmen listesinde belirtilen uygun seçmenler haricinde birisi oy kullanmaya çalıştığında akıllı sözleşme bu işlemi göz ardı edeceğinden dolayı seçme hakkı bulunmayan biri seçimde oy kullanamamaktadır. Seçme hakkı bulunan seçmenler için prosedür açık olarak belirtilmektedir.

Bunun haricinde yazarlar tarafından akıllı sözleşmede 'tx.origin' yerine 'msg.sender' ile seçmenin kimliğini saptanması gerektiğinden bahsetmişlerdir. Bu durum bir seçmeni taklit etmek üzere oluşturulmuş bir başka sözleşmenin kullanılmasının önüne geçmektedir.

Emsalsizlik: Bir başka adresden oy kullanılmak istenildiğinde sözleşme işlemin yapıldığı adresi beyaz listeden doğrulayamacağı için göz ardı edecektir. Seçmen tarafından kullanılan oy değeri akıllı sözleşme üzerinde 'msg.sender' ile kimliği saptanması ve anahtar kaydı aşamasında sadece bir defa oy anahtarı kaydı oluşturulabilmesi nedeniyle bir seçmen geçerli olan en fazla bir oy kullanabilmektedir.

Bağışlayıcılık: Sistemde bağışlayıcılık özelliğinden bahsedilmemektedir. Ancak, bir seçmen oyunu değiştirmek istiyorsa, en son oyu geçerli olacak biçimde oyunu tekrardan gönderebilmesinde, bu duruma engel olacak bir durum bulunmamaktadır. Opsiyonel olarak adilliği sağlamak amacıyla sunulan oy tercihleri $g^{x_i y_i} g^{v_i}$ değerlerinin yayınlanmadan önce özet değeri ile taahhüt edilmesi adımı ile ilgili olarak, $g^{x_i y_i} g^{v_i}$ yayınlanmadan önce seçmen taahhüdünü değiştirebilmesi için bir engel bulunmamaktadır. Ancak, değerler yayınlanmaya başladıktan sonra artık oy kullanma aşaması bitti kabul edilirse, sonuç hesaplama aşamasına kadar olan süre zarfında seçmen oyunu değiştiremeyecektir. Bu durum bağışlayıcılık gereksinimine aykırı bir durum teşkil etmemektedir.

Dayanıklılık: Kendiliğinden hesaplanan seçim sistemlerinin ortak bir problemi olarak yazarlar tarafından belirtilmiş olan problemlerden biri seçimin sonucunun hesaplanamaması (abortive issue) meselesidir. Belirtildiği üzere, eğer oyunu ($g^{x_i y_i} g^{v_i}$) gönderecek seçmen sonucu diğer herkesden önce hesaplayabildiği için sonuçtan memnun kalmazsa

oy verme işlemini tamamlamamayı tercih edebilir. Bu durumda doğal olarak seçim sonucu hesaplanamamaktadır. Belirtildiği üzere, ek bir adım eklenerek[91, 92] geriye kalan tüm seçmenlerin tam işbirliği ile sonuç tekrardan hesaplanabilmektedir, ancak bu işlemde benzer bir şekilde aynı durumda sonuç vermemektedir. Yazarlar akıllı sözleme ile seçmen katılımına teşvik oluşturacak bir emanet/iade çözümü önermişlerdir. Eğer bir seçmen oy verme süresi bitmeden oy kullanma işlemini tamamlamazsa kaporasını kaybedecektir. Ancak, seçmenin seçimi iptal ettiğinde kendisine fayda sağlayacağı durumlarda çözüm geçerli olmamaktadır.

Adillik: Oyunu son kullanan seçmen herkesten önce oyunu kullanmış gibi sistemi blokzincirde kayıtlı değerler ile simule ederek sonucu hesaplayabilmektedir. Bunun bir sonucu olarak kullanacağı oy, sonuçtan etkilenebileceği yazarlar tarafından uyarlama meselesinin(adaptive issue) kendiliğinden hesaplanabilen seçim sistemlerinin ortak bir problemlerinden biri olarak belirtilmektedir. Seçmenin kararının etkilenmemesi için opsiyonel olarak bir adım daha önerilmiştir. Bu adımda tüm seçmenler oylarını göndermeden önce kullanacakları oyun değerinin $H(g^{x_i y_i} g^{v_i})$ olacak biçimde özet değerini bildirebilmektedirler. Bu durumda en son oy kullanan seçmen sonucu önceden hesaplayabilse dahi oyunu değiştiremeyeceği için oy kullanma süreci etkilenmemektedir.

Mahremiyet: Bir seçmenin mahremiyeti oyunun gizliliğine dayanmaktadır. Oyun gizliliği ayrık logaritma problemine dayanması nedeniyle oy değerinin hesaplanarak bulunması uygulanabilir değildir. Bir seçmenin oyu yazarlar tarafından belirtildiği üzere, ancak oy kullanmış olan tüm diğer seçmenlerin oyunu açıklaması ile bulunabilmektedir. Bu nedenle sistem mahremiyet gereksinimini karşılamaktadır.

Baskı Dirençliliği: Gözetimsiz bir ortamda gerçekleştirilen bir seçim için protokolün baskı dirençliliği gösteremeyeceği yazarlar tarafından belirtilmiştir. Baskı altında oyunu kullanmak durumunda kalan bir seçmen, oyunu değiştirebiliyor olsa dahi kullandığı oyu x_i oy anahtarı değerini açıklayarak ispatlayabileceği için baskı dirençliliği sağlanamayacaktır.

Makbuzsuzluk: Bir seçmenin oy anahtarı x_i ile kullanmış olduğu oyu ispatlamak amacı ile açıklayarak blokzincir üzerinde açık olarak kayıtlı bulunan değerler ile bir makbuz oluşturabileceği yazarlar tarafından belirtilmiştir.

Bireysel Doğrulanabilirlik:

- Sunulan pusula formatının doğruluğu: Oy formatı 1 değeri evet, 0 değeri hayır olacak biçimde açık ve net olarak belirtilmiştir.
- Kullanıldığı gibi kayıt: Kullanılan oyların şifrelenmiş olarak blokzincire yazılmasından dolayı, bir seçmen oyunun doğru kayıt edilip edilmediğini blokzinciri takip ederek doğrulayabilmektedir.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu: Kullanılan oyların formatının doğruluğu oy ile birlikte gönderilen CDS sıfır bilgi ispatına[93] dayanmaktadır. Fazla ya da negatif oy kullanma girişiminde bulunan bir seçmen oy formatı ispatını oluşturamayacaktır. Bu ispatın herkes tarafından kontrol edilebiliyor olması nedeniyle bu kontrol sağlanmaktadır.
- Kayıt edildiği gibi sayılma: Önerilen sistemin kendiliğinden hesaplanabilen bir seçim sistemi olmasından dolayı, herhangi biri seçim sonucunu blokzincir üzerindeki değerleri kullanarak kendisi hesaplayabimektedir. Hesaplanan sonuç, duyurulan sonuç ile karşılaştırılarak kontrolü sağlanabilmektedir.
- Tutarlılık: Seçim verisinin blokzincir üzerinde kayıtlı tutulmasından dolayı ve kayıt edilen oylardan birinin eksik olma durumunda zaten sonucun hesaplanamamasından dolayı bu durum herhangi biri tarafından kontrol edilebilmektedir.
- Kayıt edilen her oy, ”kullanıldığı gibi kayıt” kontrolüne tabi tutulur: Şifrelenmiş olarak kullanılan tüm oylar, yönetici tarafından yayınlanan seçmen listesinde bulunan bir seçmen tarafından transfer işlemi oluşturularak kullanılmak zorundadır. Aksi bir durumda, seçim sonucu hesaplanamadığı gibi liste ile sayılan oylar karşılaştırılarak bir seçmen tarafından kullanılmamış olan oy tespit edilebilmektedir.

4.6 Polys Online Voting

Ticari olarak e-seçim hizmeti sunan Polys Online Voting [56], sıfır bilgi ispatı ile oy formatının geçerliliğini sağlarken, ortak El-Gamal açık anahtar şifrelemesi ile seçmen kimliği ve kullanılan oylar arasındaki bağı gizlemekte olan web tabanlı bir seçim sistemidir. Ethereum blokzincir altyapısını kullanmaktadır. Güvenilir seçim temsilcileri ile anahtar şifrelemsini ve sonuçların açıklanmasını sağlamaktadır. Hazırlık, kayıt, oy kullanma ve sonuç hesaplama adımlarından oluşmaktadır.

4.6.1 Hazırlık Aşaması

Hazırlık aşamasında en kritik role sahip kişiler güvenilir temsilcilerdir. Güvenilir temsilciler bir seçimdeki adaylar olabileceği gibi seçimi denetleme ile görevli gözlemcilerin de olabileceği belirtilmiştir. Blokzincirdeki blokların imzalanmasından, oylarını şifrelemesinde kullanılacak ortak anahtarın üretiminden, ve sonuçların hesaplandıktan sonra şifrelerinin çözülmesinden sorumlulardır. Bir seçimi başlatmak için her bir temsilcinin takip etmesi gereken adımlar aşağıdaki gibi belirtilmiştir.

Güvenilir temsilciler, ortak anahtar çifti Shamir sır paylaşımı [84] kullanarak kendi aralarında üretir. Her bir güvenilir temsilci üretilen anahtar çiftinin gizli değerinin bir parçasına sahip olmasından dolayı seçim sonucunun öğrenilebilmesi için eşik değerinden fazla sayıda güvenilir temsilcinin bir araya gelmesi gerekmektedir.

1. Tüm güvenilir temsilciler sistem tarafından sağlanan bir madenci/gözlemci uygulaması edinir.
2. Blokları imzalama amacı ile kullanılacak kişisel bir anahtar çifti oluştururlar.
3. Güvenilir temsilci P_i, (t, n) eşik şeması ile sistemin ortak anahtarı s oluşturulabilmesi için bir gizli anahtar s_i oluşturur.

$$s = \sum_{i}^{n} s_i$$

4. Güvenilir temsilci P_i, rastgele $k-1$ dereceden polinom f_i üretir.

$$\begin{aligned} f_i(x) &= s_i + a_{i,1} \cdot x^1 + a_{i,2} \cdot x^2 + \ldots + a_{i,(k-1)} \cdot x^{k-1} \\ &= s_i + \sum_{j=1}^{k-1} a_{i,j} \cdot x^j \end{aligned} \tag{4.1}$$

5. P_i, $0 < z \leq n$ olacak şekilde ürettiği gizli polinom üzerindeki noktaları $(z, f_i(z))$ diğer tüm temsilcilere gönderir. Ayrıca noktaları ürettiği polinom kullanılarak oluşturulduğunun kontrol edilebilmesi için $0 \leq j < k$ için $c_{i,j} = g^a_{i,j}$ değerlerini yayınlar.

6. Yayınlanan değerler, her bir temsilci tarafından kontrol edilerek doğrulanır.

$$F_{i,j} = g^{f_{i,j}} \text{ için } g^{s_i} = \prod_{l=0}^{k-1} F_{i,j}^{i^l} \tag{4.2}$$

7. Seçim ortak anahtarının açık anahtarı pk_{common}'un paylaşılan parçalar kullanılarak oluşturulduğunu kontrol etmek için şu denkliği doğrular.

$$\prod_{j=1}^{n} g^{s_i} = \prod_{j=1}^{n} F_{i,0} = pk_{common} \tag{4.3}$$

8. Eğer tüm kontroller doğrulanmış ise temsilci açık anahtarı imzalayarak anahtarın doğruluğunu gösterir.

Bu aşamada, son olarak seçime katılan her bir aday için bir asal sayı atanmaktadır.

$$Z_f = \{2, 3, 5, 7, 11, ...\}$$

4.6.2 Kayıt Aşaması

Seçmen kimlik doğrulaması problemi belirtilmekte olmakla beraber, değişen durumlar için farklı yöntemlerin kullanılabileceğinden bahsedilmiştir. Kimlik doğrulama işlemi seçimden seçime değişebileceği için bu adımın üçüncü bir parti tarafından sağlanması bu sistemin kabullerinden biridir. Seçmen kayıtlarının var olan sistemler ile entegre olacak şekilde çalışabileceği belirtilmiştir. Üç tip kayıt yöntemi bulunmaktadır. Bunlardan ilki seçmenlerin e-posta adreslerinin seçimin oluşturulurken belirtilmesi ile gerçekleşir. Sistem her seçmene özel olacak şekilde oy kullanabilecekleri bir bağlantı adresini e-posta adreslerine gönderir. İkinci olarak, seçmen sayısı seçim oluşturulurken belirtilerek her

seçmen için bir adet eşsiz kod oluşturulur. Oluşturulan kodlar seçmenlere dağıtılarak oy kullanmalarına olanak sağlanır. Son yöntem, açık olarak gerçekleştirilen konferans sırasında gerçekleşebilecek oylamalar gibi seçmenlerin önceden bilinmediği durumlar için sunulmuştur. Seçime özel bağlantı adresinden, seçmenler ilgili seçim için oy kullanabilmektedir. Açık oylama için kayıt yöntemi deneysel olarak sunulduğu belirtilerek, geniş ölçekli seçimler için uygun olmadığı belirtilmiştir.

4.6.3 Oy Kullanımı Aşaması

Oylama sürecinin en kritik parçaları oy kullanma hakkına sahip seçmenlerin anonimliğini sağlarken aynı zamanda tüm pusulaların doğru formatta olduğunundan emin olunmasıdır. Kimliği doğrulanmış bir kişi sisteme oturum açtığında eğer oy kullanma hakkına sahipse aşağıda belirtilen adımlar takip edilir.

1. İstemci uygulaması seçmen için blokzincir üzerinde transfer işlemi oluşturabilmesi amacıyla bir açık anahtar çifti üretir.
2. Seçmen tercih ettiği adayın numarası Z_i'yi ortak seçim anahtarı pk_{common} ile şifreleyerek kullanılan oyun formatının doğruluğunu ispatlamak amacıyla $SBI(\mathcal{V} \in Z_f)$ ile birlikte imzalayarak blokzincire kaydedilmesi için gönderir. Ayrıca imza oyun takibi için kullanılabilmektedir.

$$\mathcal{V} \in Z_f \text{ için } Pusula = Sign_{sk_{voter}}(Enc_{pk_{common}}(\mathcal{V})) \tag{4.4}$$

3. Güvenilir temsilcilerden herhangi biri pusulayı teslim aldıktan sonra seçmenin imzasını doğrular. Eğer imza geçerli değil ise pusula geçersiz olarak kayıt edilir.

Sistemde, SBI'nın geçerliliğini doğrulama işleminin sayım sırasında yapılması tercih edilmiştir.

4.6.4 Seçim Sonucu Aşaması

Seçmenlerin tercihlerini şifrelemede kullandığı ElGamal algoritmasının çarpımsal olarak homomorfik özelliği göstermesinden ötürü seçimin oylama süreci bittikten sonra geçerli

oylar çarpılarak seçim sonucunun temsilciler tarafından üretilen ortak seçim anahtarı pk_common ile şifrelenmiş hali elde edilebilmektedir.

$$\prod Enc_{pk_common}(\mathcal{V}_i) = Enc_{pk_common}(\prod \mathcal{V}_i)$$

Temsilciler ellerinde bulunan ortak seçim gizli anahtarı s'in parçalarını sırayla sonuca uygulayarak sonuçların şifresini çözebilirler. Elde edilen sonuç büyük adım/küçük adım algoritması ile asal çarpanlarına ayrılarak adayların almış oldukları oylar bulunur.

4.6.5 Gereksinim Analizi

Seçme Hakkı: Oy kullanımı için her seçmene özel ve spesifik olarak gönderilen bir eposta üzerinden oy kullanılabilmektedir. Sistemde her bir seçmen için KECCAK-256 özet algoritması ile üretilmiş bir eşsiz jeton değerleri akıllı sözleşmeye eklenmektedir. Eğer seçmenin oy kullanma hakkı bulunuyor ise kendileri için yeni üretilen bir aracı sözleşme ile, yada daha önce üretilmiş olan ile, kullanmakta olduğu blokzincir adresi farklı olsa dahi oy kullanılabilmektedir. Eğer sözleşmeden seçmenin jetonu bulunmamakta ise oy kullanma akıllı sözleşme tarafından kullanılan oy işlenmemektedir. Dolayısı ile sistem seçme hakkı gereksinimini sağlamaktadır.

Emsalsizlik: Her seçmen için oluşturulan seçimde takma isim olarak belirtilen özel bir aracı akıllı sözleşme bulunmaktadır. Bir seçmenin kullanmış olduğu oy durumu bu sözleşme ile takip edilebilmektedir. Akıllı sözleşmenin çıktılarının blokzincir üzerine yazılmasından dolayı, seçmen oyunu değiştirmek istediğinde önceki oyunu iptal edecek bağ kurulabilmektedir. Bu nedenle sistemde emsalsizlik gereksinimini sağlamaktadır.

Bağışlayıcılık: Emsalsizlik gereksiniminde belirtildiği üzere seçmen oyunu seçimin süresince istediği zaman değiştirebilmesine olanak sağlanmıştır.

Dayanıklılık: Seçim sonuçlarının şifresinin çözülerek sonuçların öğrenilmesine engel olabilecek anahtarın kaybı ya da gerekli işlemin yapılmasının temsilci tarafından reddedilmesi gibi durumlardan etkilenmemesi için eşik şeması kullanılarak ortak anahtar

üretilmiştir. Bu durum, eğer temsilciler uygun bir şekilde seçilmişse bahsedilen problemleri hafifletmektedir. Ayrıca sıfır bilgi ispatı algoritmasının geçerlilik(soundness) özelliğini sağladığı varsayılırsa, bir seçmenin şifrelediği oyu sıfır bilgi ispatı ispatlamasından dolayı, doğrulayıcıyı yanıltabileceği bir ispatı oluşturması hesapsal olarak uygulanabilir değildir. Seçim sonucunun öğrenilmesini engelleyebilecek durumlardan birisi de hesaplanan sonucun çok büyük olduğu durumlarda asal çarpanlarına ayrılamamasıdır. Yazarlar bu durumu belirterek, böyle bir durumda daha küçük kısmi sonuçların bir araya getirilerek hesaplanabileceğini belirtmişlerdir. Her kısmi sonuç hesabı için temsilcilerin sahip oldukları anahtarları tekrardan kullanması gerekmeksinden dolayı risk artmaktadır.

Adillik: Güvenilir temsilcilerin dürüst davrandığı varsayılırsa, kısmi seçim sonuçları oy kullanma süresi boyunca ElGamal algoritamasının açık anahtarının bilinmemesinden dolayı kimse tarafından hesaplanamamaktadır.

Mahremiyet: Seçmen mahremiyeti oyun ElGamal algoritması ile üretilen ortak anahtarın gizliliği ile korunmaktadır. Bu nedenle ortak anahtara karşılık gelen gizli anahtarın seçimden sonra da korunması gerekmektedir. Bu durum mahremiyet gerekliliğini uzun vadede riske sokmaktadır. Çünkü, gizli anahtarın ifşa edilmesi, seçimde oy kullanmış tüm seçmenlerin oyunu açık edecektir.

Baskı Dirençliliği: Baskı ve oy ticaretinin önüne geçilebilmesi için bir seçmenin birden fazla oy kullanmasına müsade edilmektedir. Ancak makbuzsuzluk özelliğinin sağlanması her zaman baskı dirençliliğinin de sağlanacağı anlamına gelmemektedir, [4]. Bir saldırgan, seçmenin sisteme oturum açma bilgilerini elde ederek baskı uygulayabilir. Ayrıca, oyunu satmak isteyen bir seçmen, sisteme giriş bilgilerini yada kendisine e-posta ile gönderilen jeton bilgisini satarak oy ticareti gerçekleştirebilir. Bu durumu engelleyecek bir mekanizmadan bahsedilmemiştir.

Makbuzsuzluk: Bir seçmen blokzincirde yayınladığı şifrelenmiş oyunu imzalamada kullanmış olduğu gizli anahtarı bildiğini göstererek oyunu göndermiş olduğu işlemi ispatlayabilir. Ancak oy değeri şifrelenmiş olacağı için kullandığı oyu da ispatlaması gerekir.

ElGamal algoritmasında seçmen tarafından üretilen geçici (ephemeral) anahtarı ile birlikte açık anahtar kullanılarak blokzincire kayıt edilmiş oyu tekrardan oluşturabileceğinden dolayı seçmen kesin bir şekilde kullanmış olduğu oy değerini ispatlayabilmektedir.

Bireysel Doğrulanabilirlik:

- Sunulan pusula formatının doğruluğu: Seçmene sunulan pusula formatının doğruluğunun kontrolünden bahsedilmemektedir.
- Kullanıldığı gibi kayıt: Seçmenin oyu blokzincirde akıllı sözleşmeler ile kayıt altına alınmasından dolayı her seçmen kendi oyunu açık imza anahtarı ile imzalamış olduğu kaydı veya aracı sözleşmesinin çıktılarını takip edebilmektedir.

Genel Doğrulanabilirlik:

- Kullanılan oyların formatının doğruluğu: Kullanılan oyların formatının doğruluğu sıfır bilgi ispatına dayanmaktadır. Herhangi biri blokzincirde yayınlanan şifreli metin ile sıfır bilgi ispatını doğrulayarak kullanılmış oyların formatının doğruluğunu kontrol edebilmektedir.
- Kayıt edildiği gibi sayılma: Ethereum blokzincirinde akıllı sözleşme sonucunda oluşan transfer işlemleri tüm düğümler tarafından defterlerine işlenerek blokzincire kayıt edilmesinden dolayı, her seçmenin oyu kayıt edildiği andan itibaren değiştirilemeyeceği için kontrol sağlanmaktadır. Burada bahsedilen değişim kayıt edilen oyun seçmenin bilgisi olmadan değiştirilemeyeceğidir.
- Tutarlılık: Herhangi biri kayıt edilen oyların formatını ve imzalarını doğrulayarak sayım sonucunda elde edilen şifreli metini elde edebilir. Eğer güvenilir temsilciler şifresini çözdükleri seçim sonuçlarının ortak anahtar ile şifrelenmiş bu şifreli metin ve kullanılarak çözüldüğünün ispatını yayınlamakta ise tutarlılık kontrolü sağlanabilirdir.
- Kayıt edilen her oy, ”kullanıldığı gibi kayıt” kontrolüne tabi tutulur: Farklı seçmenlere aynı eşsiz kod verilmesi halinde, sistemin seçmenlere adreslerini değiştirme imkanı sağlamasından dolayı bu durum herhangi biri tarafından tespit edilemeyecektir. Eşsiz kod dağıtımı ile seçmen kaydının yapıldığı seçimlerde

Bölüm 5

Blokzincir Tabanlı E-seçim Sistem Önerilerinin Uygulanabilirliği

Bu bölümde, öncelikle halihazırda kullanılmakta olan blokzincir sistemlerinin genel olarak e-seçim hazır bulunurluğu tartışılacak olup, daha sonrasında ise blokzincir tabanlı genel bir e-seçim sisteminin gerekli gereksinim kriterlerini sağladığı varsayımında bulunarak Türkiye'de gerçekleştirilecek bir seçimde tercih edilmesi halinde oluşabilecek performans maliyet analizinin kritiği yapılacaktır.

Tablo 5.1: Blokzincir tabanlı E-seçim sistemlerinin gereksinim analizleri özet tablosu

	Seçmen uygunluğu	Emsalsizlik	Bağışlayıcılık	Dayanıklılık	Adillik	Mahremiyet	Baskı Dirençliliği	Makbuzsuzluk	Oy pusulasının formatının doğruluğu	Kullanıldığı gibi kayıt	Kullanılmış oyların formatının doğruluğu	Kayıt edildiği gibi sayılma	Tutarlılık	Her kayıt edilen oy 'Kullanıldığı gibi kayıt' kontroliine tabidir	Ölçeklenebilirlik
Cruz vd.[21]	✓	✓	·	✓	–	✗	·	·	✓	✓	✓	✓	✓	✓	✗
Tarasov vd.[52]	✗	✗	·	–	·	✓	·	·	·	✓	✗	✗	✗	✗	✓
Wu vd.[53]	✓	✓	·	✗	○	✗	✗	○	·	✓	✓	✓	✓	✗	✗
Liu vd.[54]	✓	✓	·	✓	–	–	·	·	·	✓	✓	✓	✓	✓	✓
McCorry vd.[55]	✓	✓	·	–	✓	✓	○	○	✓	✓	✓	✓	✓	✓	✗
Polys Voting[56]	✓	✓	✓	✓	✓	✓[a]	✗	✗	·	?	✓	?	✓	✓	✗

✓ Sağlanıyor.
✗ İddia edilmiş ancak sağlanmıyor.
○ Öneri sunulmadan bahsedilmiş.
– Uygulanamayan bir öneri ile bahsedilmiş.
· Bahsedilmemiş ve sağlanmıyor.
? Bilgi yok.

[a] Uzun vadede mahremiyetin ifşa olma riski bulunmaktadır.

Bir önceki bölümde yapılan gereksinim analizi sonuçları Tablo 5.1'de özetlenmektedir. Burada da açıkça görülebildiği üzere maalesef blokzincir tabanlı e-seçim sistem önerileri, seçim kriterlerini tam olarak sağlayamamaktadır.

Open Vote Network [55] seçim sistemi kurul seçimleri gibi küçük ölçekli seçimlerde kullanılması için tasarlanmıştır. Tablo 5.1'de her ne kadar diğer önerilere göre daha iyi bir görünüm sergilemiş olsa da, sistem tasarımından kaynaklı olarak ulusal ölçekte bir seçimde kullanılması mümkün değildir.

5.1 E-seçim İçin Kripto Para Blokzincirlerin Hazırbulunurluğu

Blokzincir teknolojisi ilk olarak finansal bir yapı olarak tasarlanmıştır. Bitcoin, Ethereum gibi kripto paraların sağlamaya çalıştıkları kriteler e-seçim sistemleri için gerekli görülen gereksinimlerden farklılık göstermektedir. Örneğin, kripto paralarda çift harcamanın önüne geçilmesi gerekirken, e-seçim için oy kullanma hakkı bulunan bir kişinin kullandığı

en son kullanılan oy geçerli olacak şekilde tek bir oy hakkı bulunmaktadır. Benzer durumlar bu bölümde ele alınacaktır.

Ulusal seçimlerde seçmen uygunluğunun sağlanabilmesi için kişinin vatandaşlığı ve yaşı gibi sahip olduğu özellikler kimlik doğrulama ile tespit edilmelidir. Seçmen kimliğinin doğrulanması bir e-seçim sisteminde mahremiyetin ilk adımıdır. Sıfır bilgi ispatına dayalı bir dijital kimlik altyapısı ile bir seçmenin kimliği açık edilmeksizin oy kullanma hakkı bulunduğunun ispatlanabilmesi, e-seçim sistemleri açısından oldukça değerli olacaktır. Ancak, gerekli mahremiyet kriterlerini sağlamayan bir dijital kimlik altyapısı yeni sorunları da beraberinde getirebilir. Burada karşılaşılabilecek zorluklardan birisi, seçmen mahremiyetinin açık edilmeksizin seçmen uygunluğu ile birlikte emsalsizliğin beraber sağlanması olacaktır. İncelenen sistemlerde dijital kimlik doğrulama altyapısının hali hazırda bulunduğu varsayılmasına rağmen bahsedilen sistemler henüz geliştirilme aşamasında olduğundan pratik uygulamaya elverişli değildir.

İncelenen tüm e-seçim sistemlerinde kayıt işlemi dürüst olduğu varsayılan bir otorite tarafından yapılmaktadır. Bu durum, otorite tarafından sahte kimlikler oluşturularak var olmayan seçmenlerin seçimlere dahil edilebilmesine, dolayısıyla sandığa hile karıştırılma riskini doğrumaktadır. Bir e-seçim sisteminin tam anlamı ile dağıtık yapıda olabilmesi için kayıt aşamasında dürüst olmayan bir yönetici tarafından oluşturulan sahte kimliklere karşı seçmen kontrolü, seçmenlerin birbirini tanımadıkları geniş ölçekli seçimler için araştırılması gereken açık meselelerden bir diğeridir.

Bir başka mesele ise seçim maliyetlerinin düşürülmek istendiği e-seçim sistemlerinde güvenli olarak görülen hali hazırdaki kripto para ağlarından faydalanılmak istenmesi halinde işlem ücretleridir. Bitcoin ve Ethereum gibi blokzincir yapılarında uygulanan işlem ücretleri finansal bir yapı olarak ele alındığında gayet makul ve anlaşılabilirdir. Ancak bir e-seçim sisteminde seçmenin oy kullanabilmesi için az bir miktar da olsa paraya sahip olması gerekmesi, seçme hakkına aykırı bir durum oluşturmaktadır. İşlem ücretlerinin, organizatörler tarafından sağlanması halinde ise Bitcoin ve Ethereum gibi blokzincirlerde yapılan tüm transfer işlemleri her zaman tarihçeleri ile olan ilişkilerini korumaktadır, [86, 94]. Bu durum, oyların açık metin olarak gönderildiği veya sayım sırasında deşifre edildiği sistemlerde, e-seçim kriterlerinden olan seçmen mahremiyetinin, seçmenlerin seçimden önceki veya sonraki davranışlarına bağlı olarak korunamamasına neden olacaktır.

Bitcoin'in değeri 2017 Aralık ayında 19.000,00$'ın üzerine çıkması, bu çalışmanın yapıldığı sırada 10.000,00$ civarında değere sahip olması, işlem ücretlerinden kaynaklanan maliyeti ciddi oranda etkilemektedir. İşlem ücretlerine göre ilk doğrulama sürelerinin alındığı bir kripto para sisteminde, teknik olarak minimum ücret ödenmesi halinde madencilerin, oluşturulan transfer işlemlerine ilgisini azaltmakta ve bloğa eklenme süresini geçiktirebilmektedir. Düşük ücretli transfer işlemleri ile kullanılacak oyların blokzincire kaydı için ciddi bir süreye ihtiyaç duyulacaktır.

Ayrıca bir ülkenin kendi vatandaşları arasında seçim gerçekleştirmek amacıyla oluşturacağı bütçenin ülke dışında bulunan madencilere aktarılması, yeni tartışmaları da beraberinde getirecektir. Seçim maliyeti genel olarak düşürülse de, ekonomik olarak oluşabilecek problemlerin incelenmesi gerekecektir. Bu meselelerin üstesinden gelmek için çözüm önerileri oluşturulsa bile, ekonomik bir değerin seçim sistemlerinde kullanılmasının etik ve pratik olarak uygulanması tartışılmaya açık bir diğer konudur. Örneğin, ekonomik olarak değeri yüksek bir kripto para ile gerçekleştirilen seçimlerde, seçmenlerin oy kullanmaları için kendilerine iletilen parayı elinde tutmayı yada başka şekilde harcamayı tercih edebilme ihtimali bulunmaktadır. Bu demokratik olarak gerçekleştirilmek istenen ve katılımın arttırılması hedefine, dolayısıyla seçimlerin doğasına aykırı bir durum oluşturmaktadır.

Günümüzde açık izinsiz kripto para blokzincirlerinde ölçeklenebilirlik problemi bulunmaktadır. Blok oluşturma sıklığı, blok içerisinde kayıt edilen transferlerin boyutu gibi kısıtlamalar nedeni ile oluşturulabilecek maksimum işlem sayısı sınırlı olmaktadır.

Bitcoin'in bir blok oluşturma süresi oluşturulan bloğun düğümler arasında yayılabilmesi adına yaklaşık olarak 10 dakika olacak şekilde ağda bulunan düğümler tarafından kararlaştırılmaktadır. Bunun yanı sıra, her bir blok en fazla 1 mega bayt ile sınırlandırılarak merkezileşmeye karşı ağda bulunan her düğüme blok oluşturma şansı tanınmaktadır. Dolayısı ile bir bloğa eklenebilecek maksimum transfer miktarı sınırlıdır. Bitcoinin veri depolama kapasitesi, transfer başına `OP_RETURN` içersinde 80 bayt ile sınırlıdır.

Ethereum blokzincirinde akıllı sözleşmelerin çalıştırılabilmesi için gereken gaz miktarı işlem ücreti olarak karşılanmalıdır. Kriptografik fonksiyonların hesapsal olarak normalde gerçekleştirilen işlemlere göre fazla işlem gerektirmesinden dolayı, akıllı sözleşme içerisinde kullandıldıklarında gaz maliyetini oldukça arttırmaktadırlar. Maliyet artışının

haricinde Ethereum blokzincirinde akıllı sözleşmelerde kısıtlama olarak bir blok içerisinde ve bir transfer işleminde ayrı ayrı var olan maksimum harcanabilecek gaz kısıtlamalarından dolayı homomorfik hesaplamalar yada sıfır bilgi ispatı gibi bazı işlemlerin henüz yapılamadığı belirtilmiştir, [55].

Blokzincirin sağlamakta olduğu en büyük faydalardan biri olan dağıtık olarak güvenilir transfer işleminin yapılabilmesini sağlayan özelliği, yapılan işlemlerin değiştirilemiyor oluşudur. Bu özellik, genel olarak e-seçim sistemleri kapsamında açık ilan tahtası olarak oyların değiştirilmediğinin doğrulanması için kullanılmaktadır. Blokzincirde kullanılan mutabakat mekanizmasına göre değişebilen dürüst olmayan düğüm toleransı, kullanılan mutabakatın kriterleri yerine getirildiğinde geçerlidir. Örneğin, işlem gücüne dayalı işlem ispatı mutabakatında hesaplama gücünün yarısından fazlası dürüst olursa blokzincirde yapılan işlemler blokzincirden silinemeyecektir. %51 atak olarakda bilinen, hesaplama gücünün merkezileşmesi probleminin genel olarak incelenen sistemlerde gerçekleşmeyeceği varsayılmaktadır. Ancak yapılan bir araştırmaya göre, Bitcoin madenci düğümlerinin sadece yüzde 2'si toplam hesaplama gücünün 3/4'ünü oluşturduğu belirtilmiştir, [95]. Politik olarak değer taşıyan seçim sistemlerinde, mutabakatın güvenliğini sağlayan kaynağın çoğunluğunu elinde bulunduran kişiler tarafından seçimlere manipülasyon uygulanması teknik olarak mümkün olabilmektedir. Merkezileşmiş bir hesaplama gücünün e-seçim kapsamında, kayıt altına alınmış bir oyun sonuca dahil edilmeden defterden silinebileceği anlamını taşımaktadır. Ulusal bir seçimde, seçmenin kullanmış olduğu oyun güvenli olarak kayıt altına alındığının söylenebilmesi için merkezileşmeye karşı alınması gereken önlemler blokzincir ile tasarlanan sistem kapsamında göz önünde bulundurulmalıdır. Örneğin, normal şartlar altında Bitcoin kripto parasında transfer işleminin blokzincirde doğrunabilmesi için minimum 2 ile 6 arasında doğrulama alınması gerekmektedir. Bu miktarın bir e-seçim sistemi için daha fazla olması beklenmektedir. Ancak bu önlemin dezavantajı olarak bir oyun kayıt süreci süre olarak uzamakta ve seçmen açısından kullanılabilirliği negatif olarak etkilenmektedir.

Blokzincir tabanlı e-seçim sistem önerilerinde kullanıcı cihazları güvenli kabul edilmektedir. Ancak, ulusal bir seçimde oy kullanan seçmenlerin kullanmış oldukları cihazların güvenliğinin sağlanması açık kalan bir başka problemdir. Bunun yanı sıra, seçmenler arasında e-seçim yöntemlerini tercih etmeyenler yada imkanı olmayan kişiler için blokzincir tabanlı e-seçim sistemi ile birlikte kağıt tabanlı seçimin bir arada sunulması da genel olarak göz ardı edilen meselelerden biridir.

5.2 Mevcut Önerilerin Türkiye seçimlerine Uygulanabilirliği

Türkiye'de gerçekleştirilen en son ulusal seçimde belirtildiği üzere yaklaşık olarak 57 milyon seçmenin oy kullanma hakkı bulunmaktadır, [2]. Bu bölümde, bu sayı baz alınarak takribi olarak maliyet ve süre hesapları yapılarak uygulanabilirlikleri incelenecektir.

5.2.1 Bitcoin Tabanlı E-seçim Sistemleri

Bitcoin'de dahil edilen girdi ve çıktılara göre transfer işleminin boyutu değişebilmektedir. Bir girdi ve iki çıktıdan oluşan basit bir transfer işlemi yaklaşık olarak 250 bayt veri barındırmaktadır. Maksimum blok büyüklüğünün boyut olarak 1 megabayt ile sınırlandırılmasından dolayı bir blok içerisine en fazla 4000 transfer işlemi eklenebilmektedir. İşlem gücünün ispatı mutabakatının zorluk derecesinden dolayı bir blok oluşturma süresi yaklaşık olarak 10 dakikadır. Seçmenlerin oluşturduğu transfer işlemine öncelik verildiği en iyi durumda saatte en fazla 24000 transfer işlemi kayıt altına alınabilecektir.

E-seçim sistemi kapsamında tüm seçmenler tarafından oluşturulan transfer işlemlerinin işlenebilmesi için transfer başına yaklaşık 14250 adet blok oluşturulması gerekmektedir. Yaklaşık olarak 10 dakikada bir blok oluşturulduğu varsayılırsa, bu kadar bloğun oluşturulması minimum 99 gün sürecektir. Oy kullanımı için yapılması gereken işlem sayısı arttıkça, bu rakamın her transfer işlemi ile kümülatif olarak arttığının belirtilmesi gerekmektedir. Örneğin bir adet kayıt için, bir adetde oy kullanımı için transfer işlemi yapıldığı bir sistemde bu süre yaklaşık olarak 198 gün olacaktır. Önemle belirtilmesi gerekir ki, bu durum transferlerin fazlada bir veri barındırmadığı ve ağdaki madencilerin e-seçim transferlerine öncelik verdiği en iyi durum senaryosu, yani sadece seçmenlerin oyunun kayıt edildiği göz önüne alınarak elde edilmiştir.

Bitcoin'de işlem ücretleri transferi oluşturan kişi tarafından belirlenir. İşlem ücreti miktarı sadece ilk doğrulamanın ne kadar hızlı alındığını etkilemektedir. İşlem ücreti miktarı, işlemin blokzincire eklenmesi ile ilk doğrulamanın alınması süresine göre belirlenir. Bu miktar günlük işlem yoğunluğuna göre değişebilmektedir. Tablo 5.2'de belirtilen işlem ücretleri, 19.08.2019 tarihi baz alınarak verilmiştir. Dipnot olarak, Bitcoin'de bir işlemin geçerli olarak işlenmesi için 2 ile 6 arasında doğrulama beklenilmesi tavsiye edilmektedir.

Tablo 5.2: Transferin bloğa eklenmesi için gereken blok zamanı ve yaklaşık işlem ücretleri [96]

İlk Doğrulama Bloğu	Tahmini Süre	Tahmini İşlem Ücreti	Tahmini İşlem Ücreti(USD)
İlk blok	10 dakika	33 satoshi/bayt	0.85$
3. blok	30 dakika	32 satoshi/bayt	0.82$
6. blok	1 saat	9 satoshi/bayt	0.25$

Oy kullanımı sırasında oluşturulan yaklaşık 250 bayt büyüklüğü sahip bir transfer işleminin ilk doğrulanmasını ilk blok içerisinde elde edilmesi için bayt başına 33 satoshi işlem ücreti verilmelidir. Toplamda bir trasfer işlemi 8250 satoshi (0.85$) işlem ücreti ödenmesi gerekmektedir. İlk doğrulama alındıktan sonra yaklaşık olarak 1 saat süre içerisinde 6 adet doğrulama alınabileceği için toplamda yaklaşık olarak 70 dakikalık süreye ihtiyaç bulunmaktadır.

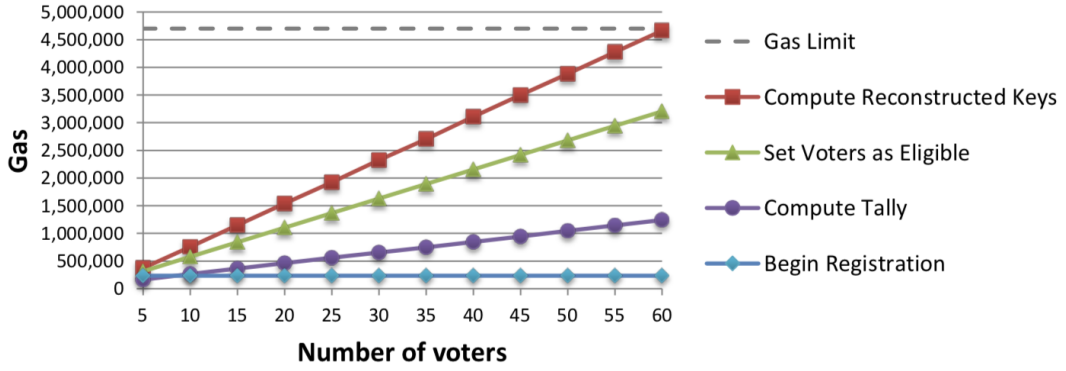
Türkiye'de gerçekleştirilmek istenen bir seçim için her seçmenin 70 dakika içerisinde oyunun blokzincirde yeterli doğrulamayı alabilmesi için toplamda yaklaşık olarak 4702,5 BTC (47 milyon dolar) bir seçim maliyeti oluşturulmalıdır. Bu miktar bir seçmenin oy kullanımı için yapması gereken transfer işlemi sayısı ile birlikte kümülatif olarak artmaktadır. Ayrıca transfer işlemi ücreti madencilere gönderilecek olması nedeni ile bu miktar her seçim için tekrardan oluşturulmak durumundadır. Bu maliyet oy kullanımı için 1 transfer işlemi gerçekleştirildiğinde yaklaşık olarak hesaplanmıştır.

5.2.2 Ethereum Tabanlı E-seçim Sistemleri

Bitcoin, her ne kadar bir e-seçim sistemi için gerekli olan açık ilan tahtasının sağlaması beklenilen değiştirilememe özelliği ile birlikte doğrulanabilirliği sağlıyor olsa da sınırlı veri depolayabilme kabiliyeti bulunmaktadır. Bunun haricinde Bitcoin'in betik dili Turing bütünlüğünü sağlamaması nedeniyle yapılabilecek işlemler kısıtlıdır. Daha detaylı olarak Bitcoin betik dili sınırlı bir alana sahip olmakta ve döngüleri desteklememektedir. Bu çalışmada yapılan analizlerde her ne kadar seçim protokolünün dürüst olarak gerçeklendiği varsayılmış olsa da, protokolün işletilmesi doğrulanabilir olmalıdır. Ethereum, Bitcoin'in aksine veri barındırabilmekle beraber akıllı sözleşme adı verilen programları üçüncü partilere ihtiyaç duyulmaksızın tüm ağda doğrulanabilecek şekilde işletebilmektedir.

Ethereum tabanlı e-seçim sistemlerinde, çalıştırılan programların sonlandırıldığından emin olmak için yapılan her işlem belirli bir miktar gaz ödemesi gerektirmektedir. Bu

gereklilik aynı zamanda işlem ücretlerinin hesaplanmasında da kullanılmaktadır. Ethereum ağı, kullanıcılar tarafından kullanılabilecek gaz miktarını sınırlanmasından dolayı sıfır bilgi ispatı, homomorfik şifreleme gibi fazla hesaplama gerektirebilen bazı işlemleri akıllı sözleşme üzerinde yapılabilmesine imkan sağlamamaktadır, [55]. Bu durumda OVN e-seçim sisteminin dayanıklılık gösterdiği varsayılmış olsa dahi Ethereum üzerinde bir e-seçim protokolünün ulusal seçimlerde kullanılmak üzere işletilmesi mümkün değildir.



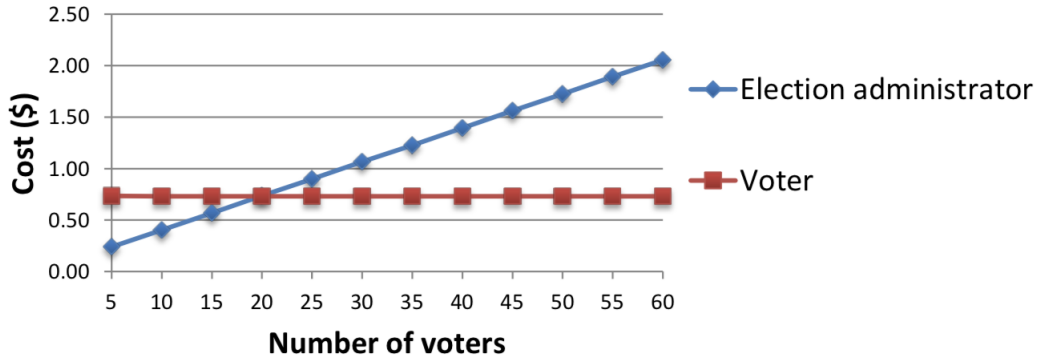
Şekil 5.1: OVN Seçmen sayısı ve gaz limiti grafiği[55].

Open Vote Network'de belirtildiği üzere kurulum aşamasında anahtarların yeniden hesaplanması sırasında Ethereum gaz limitine yaklaşık 60 adet anahtar kullanıldığında erişilmektedir. Gaz limitine erişildiğinde akıllı sözleşme tamamlanmamış olmasına rağmen işlem ücreti kesildiği için güvenli limit 50 olarak belirtilmiştir. Şekil 5.1 üzerinde görülebildiği üzere sistemin bir bütün olarak ölçeklenebilmesi mümkün değildir.

Tablo 5.3: OVN ile 40 kişilik bir seçim için oluşturulan seçim maliyeti tablosu[55]. (Gaz Ücreti = 0.00000002 ether, 1 ether = 11$)

	Maliyet(Gaz)	Maliyet($)
Seçim Yürütücü Toplamı (Seçim başı)	12.436.190	2,74
Seçmen Başına Toplam Maliyet (Kişi başı)	3.323.642	0,73
Seçim Toplamı(40 Kişi)	145.381.858	31,98

Şekil 5.2'de görülebildiği üzere seçim maliyeti seçmen sayısı arttıkça seçim otoritesinin maliyeti artarken, seçmenlere oluşan maliyet değişmemektedir. Türkiye'de seçmenlerin 40 kişilik gruplara bölünerek Ethereum blokzinciri üzerinde OVN kullanılması ile bir seçim yapılmak istendiğinde kabaca 45 milyon dolar civarından bir maliyet oluşmaktadır.

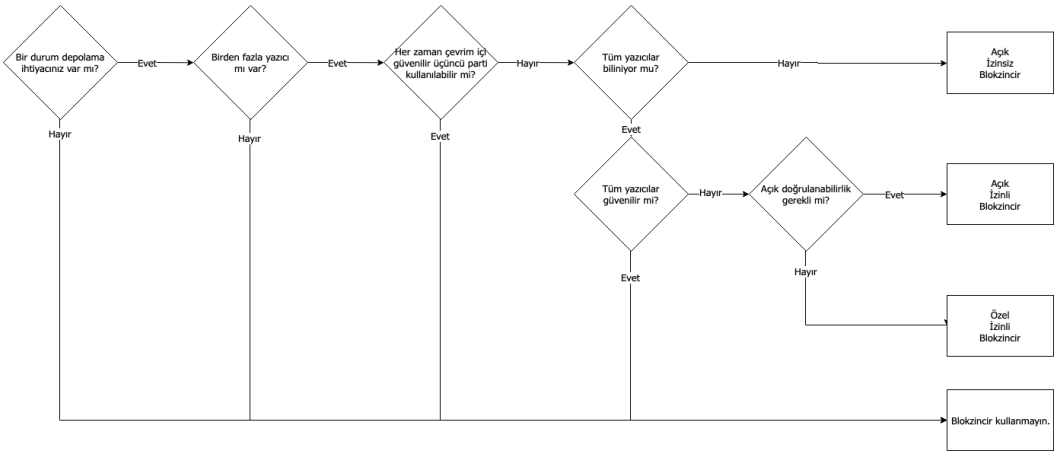


Şekil 5.2: OVN Seçmen başına maliyet grafiği[55].

Ethereum blokzincirinde, blok gaz limiti bir blokta kullanılabilecek maksimum gaz miktarını belirtir. Blok gaz limiti, bir bloğa eklenen transferlerin miktarını kısıtlayarak blokların yayılma ve oluşturulma süresini minimuma çekmek için kullanılmaktadır. Bunun yanı sıra, birbirini çağıran akıllı sözleşmeler ile etkili sonsuz döngü oluşturulmasını engellerler. Oluşturulan her blokta bu limit değişmektedir. Yaklaşık olarak 8.000.000 gaz civarındadır. Kriptografik hesaplamaların maliyetli olması nedeniyle bir blokta en fazla 6 seçmen kaydı veya bir oy kullanımı yapılabildiği belirtilmiştir, [55]. Tablo 5.3'deki veriye göre, Ethereum blokzincirinde yaklaşık 15 saniyede bir blok oluşturulduğu varsayılırsa, Türkiye'de gerçekleştirilmek istenen bir seçimde sadece seçmenlerin kaydı yaklaşık olarak 4.5 sene sürecektir.

5.2.3 E-seçime Özel Tasarlanmış Blokzincir Tabanlı E-seçim Sistemleri

Bitcoin ve Ethereum'un ölçeklenebilirlik problemleri bulunmaktadır. Tasarımlarından kaynaklanan işlem ücretlerinden dolayı maliyet artışı, hesaplama ve depolama sınırları ve blok oluşturma kısıtlamaları gibi sınırlandırmalardan dolayı ulusal düzeyde bir e-seçim gerçekleştirilebilmesine olanak vermemektedir. Bahsedilen kısıtlamalar, genel olarak kullanılan blokzincirin bir finansal yapı olarak tasarlanmış olmasından kaynaklanan kısıtlamalar olduğu göz önüne alınırsa e-seçim sistemi için daha spesifik ve özelleşmiş bir blokzincir ağı oluşturulmak istenmesi makuldur. Ancak bu durumda Bitcoin ve Ethereum'da halihazırda bulunan mutakat mekanizmasının güvenliğinin sağlanması ve blokzincir tipi gibi bazı durumların güvenlik açısından göz önüne alınması gerekmektedir.



Şekil 5.3: İş modelinizde blokzincir kullanma ihtiyacınız var mı?[49]

Wüst ve arkadaşları tarafından yayınlanan iş modelinde blokzincir ihtiyacı hakkındaki makalesinde blokzincir ihtiyacı için şekil 5.3'deki gibi bir formül sunulmuştur, [49]. Formüle göre e-seçim sistemlerinin sağlaması istenilen özellikleri göz önüne alındığında sistemde yazıcıların seçilmesine göre iki farklı tip blokzincir kullanılma potansiyeli bulunmaktadır. Açık izinli blokzincir veya açık izinsiz blokzincir.

Bunlardan ilki tüm yazıcıların bilindiği izinli blokzincir kullanılmasıdır. İzinli blokzincir oluşturulması durumunda, blokzincire yazma hakkı bulunan düğümlerin seçimi gerekmektedir. Yazma hakkı verilen düğümlerin bir merkezi otorite tarafından tanımlanır. Demokratik bir seçim ortamında bu düğümleri seçme görevi dürüst olarak yerine getirildiği varsayılsa da merkezileşmeden kaynaklanan problemler açığa çıkmaktadır. Sınırlı sayıda düğüm tarafından kontrol edilen bir blokzincir, ağda yazma hakkı bulunan düğümleri DDoS saldırılarına karşı açıkta bırakmaktadır. Seçimlerin merkezi olarak yürütülmesi her ne kadar istenmeyen bir durum olsa da, izinli bir blokzincir ağında hisse ispatı gibi daha verimli mutabakat mekanizmalarının kullanılmasını kolaylaştırmaktadır.

Diğer seçenek ise herhangi birinin bir düğüm olarak ağa dahil olabildiği, deftere yazma ve okumanın açık ve izinsiz olarak sunulduğu blokzincir tipidir. Düğümler arasında senkronizasyonu sağlarak tek bir defter oluşturulmasını ve çifte harcamanın önüne geçildiği bir mutabakat mekanizması e-seçim sistemi kapsamındaki kurallar ile tasarlanma olanağına sahip olacaktır. Bitcoin ve Ethereum'da kullanılan işlem ispatı gibi hesaplama gücüne veya hafızaya dayalı bir mutabakat mekanizması göz önüne alındığında, blokzincirin güvenliği ağ tarafından sağlanan kaynak kadar güvenli olacaktır. Öyle ki, literatürde %51 atak olarak adı geçen bir saldırganın ağda bulunan kaynağın yarısından fazlasına

sahip olma durumunda defter yeniden oluşturarak yapılan transfer işlemlerinin geri alınabilmesi uygulanabilir bir atak olma ihtimali oluşmaktadır. Seçmenler tarafından oluşturulan imzalı transfer işlemlerini değiştiremese dahi seçim sonuçları etkileneceğinden ötürü seçimin bütünlüğünün bozulma riski bulunmaktadır.

Bölüm 6

Sonuç ve Tartışma

Bu çalışmada dikkat çekici özellikleri bulunan bir teknoloji olan blokzincir tabanlı e-seçim sistemlerinin gereksinim, güvenlik ve mahremiyet analizleri yapılmıştır. Blokzincir teknolojisinin elektronik seçim alanında yeni bir dönem olması ile beraber, doğrudan demokrasiye atılan önemli bir adım olma potansiyeline sahip olduğu düşünülmektedir. Tablo 5.1'da görülebileceği üzere blokzincir tabanlı e-seçim sistemleri bir seçimin doğrulanabilirliğini sağlayabilmesinin yanı sıra e-seçim gereksinimleri açısından olgunlaşmadığı anlaşılmaktadır.

Güvenli olarak kabul edilen Bitcoin, Ethereum, Zcash gibi yüksek düğüm katılımına sahip açık izinsiz kripto para blokzincirlerinin ulusal ölçekli e-seçim sistemleri için kullanılması mümkün görünmemektedir. Bu duruma neden olan başlıca kısıtlamalar, bölüm 5'de tartışıldığı üzere izinsiz tipte finansal bir yapı olarak tasarlanmalarından kaynaklanmaktadır. Ekonomik bir değer olarak sağlanması istenilen kriterler için tasarlanmış olmaları nedeniyle e-seçim gereksinimlerinin tam ve eksiksiz olarak sağlanamıyor oluşuna başlıca sebep olarak gösterilebilir.

Gelecek çalışmalarda, seçmen uygunluğunun mahremiyet ile birlikte sağlanabilmesi için kimlik doğrulama sistemlerinin geliştirilmesi, kayıt sırasında dürüst olmayan otoritenin tespiti, ölçeklenebilirlik için e-seçim kapsamında tasarlanmış izinli bir yapıda daha verimli bir mutabakat mekanizması tasarlanması konuları e-seçim kapsamında önem arz eden meselelerdir.

E-seçim sistemleri için blokzincir kullanımının avantajları olduğu gibi dezavantajları da olduğu ve konunun e-seçim kapsamında daha derin çalışılması gerekmektedir. Genel olarak önerilen seçim sistemlerinin blokzincir teknolojisinin dağıtık yapıda oluşu, sağladığı şeffaflık, kayıtların değiştirilemez oluşu ve doğrulanabilirliği e-seçim açısında önem arz eden özellikleri vurgulamakta olmasına rağmen, beraberinde doğabilecek problemlere detaylı olarak değinilmemektedir. Bu nedenle, e-seçim spesifik blokzincir sistem tasarımları araştırılması gereken bir konudur.

Kaynaklar

[1] P. D. Webb and E. Heinz. Election, 2019, (accessed 05.2019). URL https://www.britannica.com/topic/election-political-science.

[2] T.C. Yüksek Seçim Kurulu. T.C. Yüksek Seçim Kurulu, SSS, 2019, (accessed 05.2019). URL http://ysk.gov.tr/tr/sss/1523.

[3] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In *STOC*, volume 94, pages 544–553, 1994.

[4] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 61–70, New York, NY, USA, 2005. ACM.

[5] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology — AUSCRYPT '92*, pages 244–251, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[6] P. YA Ryan, D. Bismark, J. H.r, S. Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE transactions on information forensics and security*, 4(4):662–673, 2009.

[7] S. Popoveniuc and B. Hosp. An introduction to punchscan. In *IAVoSS workshop on trustworthy elections (WOTE 2006)*, pages 28–30. Robinson College United Kingdom, 2006.

[8] R. Rivest. The threeballot voting system. 2006.

[9] R. Montjoy. The changing nature... and costs... of election administration. *Public Administration Review*, 70(6):867–875, 2010.

[10] G. Qadah and R. Taha. Electronic voting systems: Requirements, design, and implementation. *Computer Standards & Interfaces*, 29(3):376–386, 2007.

[11] D. Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[12] A. Prosser and R. Krimmer. *Electronic Voting in Europe-Technology, Law, Politics and Society*. Ges. für Informatik, 2004.

[13] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*, pages 27–40, May 2004. doi: 10.1109/SECPRI.2004.1301313.

[14] D. Gritzalis. *Secure electronic voting*, volume 7. Springer Science & Business Media, 2012.

[15] L. Fouard, M. Duclos, and P. Lafourcade. Survey on electronic voting schemes. *supported by the ANR project AVOTÉ*, 2007.

[16] B. Adida. Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335–348, 2008.

[17] T. Moura and A. Gomes. Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, pages 574–575. ACM, 2017.

[18] L. Carter and F. Bélanger. Internet voting and political participation: An empirical comparison of technological and political factors. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 43(3):26–46, 2012.

[19] T. Lauer. The risk of e-voting. *Electronic Journal of E-government*, 2(3):177–186, 2004.

[20] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb. Decentralized voting platform based on ethereum blockchain. In *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, pages 1–6. IEEE, 2018.

[21] J.P. Cruz and Y. Kaji. E-voting system based on the bitcoin protocol and blind signatures. *IPSJ Transactions on Mathematical Modeling and Its Applications*, 10 (1):14–22, 2017.

[22] P. A.D. Rezende. Electronic voting systems–is brazil ahead of its time. *RSA CryptoBytes*, 7(2), 2004.

[23] Ü. Madise and T. Martens. E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. *Electronic voting*, 86(2006), 2006.

[24] J. Gerlach and U. Gasser. Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, 3:2009, 2009.

[25] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. Attacking the washington, dc internet voting system. In *International Conference on Financial Cryptography and Data Security*, pages 114–128. Springer, 2012.

[26] I. S. G. Stenerud and C. Bull. When reality comes knocking norwegian experiences with verifiable electronic voting. In *5th International Conference on Electronic Voting 2012 (EVOTE2012)*. Gesellschaft für Informatik eV, 2012.

[27] N. Goodman. Internet voting in a local election in canada. In *The Internet and Democracy in Global Perspective*, pages 7–24. Springer, 2014.

[28] J. A. Halderman and V. Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity*, pages 35–53. Springer, 2015.

[29] S. J. Lewis, O. Pereira, and V. Teague. Ceci n'est pas une preuve. 2019.

[30] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman. Security analysis of the estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715. ACM, 2014.

[31] D.F. Aranha, P. Y. S. Barbosa, T. N.C. Cardoso, C.L. Araújo, and P. Matias. The return of software vulnerabilities in the brazilian voting machine. *Computers & Security*, 2019.

[32] L. F. Cranor and R. K. Cytron. Sensus: a security-conscious electronic polling system for the internet. In *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, volume 3, pages 561–570 vol.3, Jan 1997.

[33] O. Cetinkaya and D. Cetinkaya. Towards secure e-elections in Turkey: Requirements and principles. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 903–907, April 2007.

[34] S. Popoveniuc, J. Kelsey, A. Regenscheid, and P. Vora. Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE'10)*, pages 1–16, Berkeley, CA, USA, 2010. USENIX Association. URL https://www.usenix.org/legacy/event/evtwote10/tech/full_papers/Popoveniuc.pdf.

[35] J. Benaloh, R. Rivest, P. Ryan, P. Stark, V. Teague, and P. Vora. End-to-end verifiability. arXiv preprint arXiv:1504.03778, 2015.

[36] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008. (Accessed: 2019-02-18).

[37] D. Jayasinghe, S. Cobourne, K. Markantonakis, R.N. Akram, and K. Mayes. Philanthropy on the blockchain. In *IFIP International Conference on Information Security Theory and Practice*, pages 25–38. Springer, 2017.

[38] Binance. Binance charity, 2019, (accessed 06.2019). URL https://www.binance.charity/.

[39] S. Abeyratne and R. Monfared. Blockchain ready manufacturing supply chain using distributed ledger. 2016.

[40] F. Tian. An agri-food supply chain traceability system for china based on rfid & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)*, pages 1–6. IEEE, 2016.

[41] K. Korpela, J. Hallikas, and T. Dahlberg. Digital supply chain transformation toward blockchain integration. In *proceedings of the 50th Hawaii international conference on system sciences*, 2017.

[42] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40(10):218, 2016.

[43] A. Ekblaw, A. Azaria, J. Halamka, and A. Lippman. A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference*, volume 13, page 13, 2016.

[44] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu. The blockchain-based digital content distribution system. In *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, pages 187–190. IEEE, 2015.

[45] M. O'Dair et al. The networked record industry: how blockchain technology could transform the consumption and monetisation of recorded music. 2016.

[46] A. Dorri, S. S Kanhere, and R. Jurdak. Towards an optimized blockchain for iot. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 173–178. ACM, 2017.

[47] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pages 618–623. IEEE, 2017.

[48] S. Huh, S. Cho, and S. Kim. Managing iot devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*, pages 464–467. IEEE, 2017.

[49] K. Wüst and A. Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.

[50] Z. Zhao and H. Chan. How to vote privately using bitcoin. In *International Conference on Information and Communications Security*, pages 82–96. Springer, 2015.

[51] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474, May 2014. doi: 10.1109/SP.2014.36. URL https://doi.org/10.1109/SP.2014.36.

[52] P. Tarasov and H. Tewari. Internet Voting Using Zcash. Cryptology ePrint Archive, Report 2017/585, 2017. https://eprint.iacr.org/2017/585.

[53] Y. Wu. An e-voting system based on blockchain and ring signature. *Master. University of Birmingham*, 2017.

[54] Y. Liu and Q. Wang. An e-voting protocol based on blockchain. Cryptology ePrint Archive, Report 2017/1043, 2017. https://eprint.iacr.org/2017/1043.

[55] P. McCorry, S. F Shahandashti, and F. Hao. A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security*, pages 357–375. Springer, 2017.

[56] R. Alyoshkin. Polys online voting system. whitepaper. URL https://polys.me/assets/docs/Polys_whitepaper.pdf.

[57] A. B. Ayed. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09, 2017.

[58] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu. Large-scale election based on blockchain. *Procedia Computer Science*, 129:234 – 237, 2018.

[59] F. S. Hardwick, R. N. Akram, and K. Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. *CoRR*, abs/1805.10258, 2018.

[60] F. Þ Hjálmarsson, G. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson. Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986. IEEE, 2018.

[61] C. K. Adiputra, R. Hjort, and H. Sato. A proposal of blockchain-based electronic voting system. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 22–27. IEEE, 2018.

[62] Follow my vote (2018), 2018, (accessed 04.2019). URL https://followmyvote.com/.

[63] Xo.1 secure vote, (accessed 04.2019). URL https://secure.vote/.

[64] Votem castiron whitepaper., (accessed 04.2019). URL https://www.votem.io/#whitePaper.

[65] Voatz., (accessed 04.2019). URL https://voatz.com/.

[66] Horizon state (2017), 2017, (accessed 04.2019). URL https://horizonstate.com/horizon_state_white_paper.pdf.

[67] Agora. agora - bringing our voting systems into the 21st century v0.2., (accessed 04.2019). URL https://agora.vote/Agora_Whitepaper_v0.2.pdf.

[68] J. Cucurull, A. Rodríguez-Pérez, T. Finogina, and J. Puiggalí. Blockchain-based internet voting: Systems' compliance with international standards. In Witold Abramowicz and Adrian Paschke, editors, *Business Information Systems Workshops*, pages 300–312, Cham, 2019. Springer International Publishing. ISBN 978-3-030-04849-5.

[69] S. Gajek and M. Lewandowsky. Trustless, censorship-resilient and scalable votings in the permission-based blockchain model.

[70] B. Shahzad and J. Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, 7:24477–24488, 2019.

[71] R. Tso, Z. Liu, and J. Hsiao. Distributed e-voting and e-bidding systems based on smart contract. *Electronics*, 8(4):422, 2019.

[72] İnsan Hakları Evrensel Bildirgesi. İnsan Hakları Evrensel Bildirgesi, (accessed 04.2019). URL http://www.unicankara.org.tr/doc_pdf/h_rigths_turkce.pdf.

[73] Bitcoin. Bitcoin Wiki Documentation, 2018, (accessed 03.2018). URL https://en.bitcoin.it/wiki/Bitcoin.

[74] K. Okupski. Bitcoin developer reference. In *Eindhoven*. 2014.

[75] N. Szabo. The idea of smart contracts. *Nick Szabo's Papers and Concise Tutorials*, 6, 1997.

[76] V. Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3:37, 2014.

[77] G. Wood. Ethereum yellow paper. *Internet: https://github. com/ethereum/yellowpaper,[Oct. 30, 2018]*, 2014.

[78] M. Alan. Turing. on computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London mathematical society*, 42(2):230–265, 1936.

[79] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[80] W. Diffie and M. Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[81] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 552–565, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg. ISBN 978-3-540-45682-7.

[82] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.

[83] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

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

[85] S. Heiberg, I. Kubjas, J. Siim, and J. Willemson. On trade-offs of applying block chains for electronic voting bulletin boards. *E-Vote-ID 2018*, page 259, 2018.

[86] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[87] Zcash user documentation, viewing key, 2018, (accessed 04.2018). URL https://buildmedia.readthedocs.org/media/pdf/zcash/latest/zcash.pdf.

[88] J. K. Liu and D. S. Wong. Solutions to key exposure problem in ring signature. *IJ Network Security*, 6(2):170–180, 2008.

[89] F. Hao, P. Ryan, and P. Zieliński. Anonymous voting by two-round public discussion. *IET Information Security*, 4(2):62–67, 2010.

[90] C.P. Schnorr. Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology*, pages 239–252. Springer, 1989.

[91] A. Kiayias and M. Yung. Self-tallying elections and perfect ballot secrecy. In *International Workshop on Public Key Cryptography*, pages 141–158. Springer, 2002.

[92] D. Khader, B. Smyth, P. Ryan, and F. Hao. A fair and robust voting system by broadcast. *Lecture Notes in Informatics (LNI), Proceedings-Series of the Gesellschaft fur Informatik (GI)*, pages 285–299, 2012.

[93] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Annual International Cryptology Conference*, pages 174–187. Springer, 1994.

[94] M. Moser. Anonymity of bitcoin transactions. 2013.

[95] A. E. Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. G. Sirer. Decentralization in bitcoin and ethereum networks. *arXiv preprint arXiv:1801.03998*, 2018.

[96] Bitcoin Transaction Fees, 2019, (accessed 19.08.2019). URL https://bitcoinfees.info.