İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BLOKZİNCİR TABANLI ELEKTRONİK SEÇİM SİSTEMİ MODELLEMESİ

YÜKSEK LİSANS TEZİ

Doğa Barış ÇAKMAK

Bilişim Uygulamaları Anabilim Dalı

Bilişim Uygulamaları Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA

HAZİRAN 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

BLOKZİNCİR TABANLI ELEKTRONİK SEÇİM SİSTEMİ MODELLEMESİ

YÜKSEK LİSANS TEZİ

Doğa Barış ÇAKMAK
(708161006)

Bilişim Uygulamaları Anabilim Dalı

Bilişim Uygulamaları Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA

HAZİRAN 2019

İTÜ, Bilişim Enstitüsü'nün 708161006 numaralı Yüksek Lisans Öğrencisi Doğa Barış ÇAKMAK, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "BLOKZİNCİR TABANLI ELEKTRONİK SEÇİM SİSTEMİ MODELLEMESİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Ertuğrul KARAÇUHA** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Oğuzhan KÜLEKÇİ** İstanbul Teknik Üniversitesi	.....
	Prof. Dr. Hülya ŞAHİNTÜRK İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : **3 Mayıs 2019**
Savunma Tarihi : **12 Haziran 2019**

Eşime ve aileme,

ÖNSÖZ

Yüksek lisans eğitimim ve tez süresi boyunca hiçbir konuda yardımını esirgemeyen danışmanım Prof. Dr. Ertuğrul KARAÇUHA'ya çok teşekkür ederim.
Zorlu ve uzun bir maraton olan yüksek lisans eğitimi süresince beni destekleyen aileme, eşime ve arkadaşlarıma destekleri için teşekkür ederim.

Aralık 2018

Doğa Barış Çakmak
(Bilgisayar Mühendisi)

İÇİNDEKİLER

Sayfa

KISALTMALAR

SWOT	**: S**trengths, Weaknesses, Opportunities, Threats.
PoW	**:** Proof of Work
PoS	**:** Proof of Stake
BFT	**:** Byzantine Fault Tolerance
PBFT	**:** Practical Byzantine Fault Tolerance
DHS	**:** The Department of Homeland Security
TPS	**:** Transaction Per Second
RSA	**:** Rivest, Shamir, & Adleman
UML	**:** Unified Modeling Language

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

BLOKZİNCİR TABANLI ELEKTRONİK SEÇİM SİSTEMİ MODELLEMESİ
ÖZET

İnsanoğlu topluluk olarak yaşamaya başladığından beri karar alma mekanizması olarak seçimleri kullanmaktadır. Antik Yunan'da ve Roma'da seçimler yapılmasına rağmen modern anlamda ilk seçimler Kuzey Amerika'da ve Avrupa'da temsili hükümetlerin seçilmesiyle ortaya çıkmaktadır. Teknolojinin gelişmesiyle beraber geçmişten günümüze seçim sistemi teknolojileri de gelişim göstermiştir. Oyların palmiye yapraklarına işaretlenmesi gibi ilkel yöntemlerle başlayan bu süreç, günümüzde elektronik oy makinaları ve internet üzerinden oylama gibi teknolojik yöntemlerle yürütülmektedir.

Seçim sistemleri tasarlanırken demokratik kıstaslara uygun olması beklenmektedir. Günümüzde yaygın olarak kullanılan seçim sistemleri çeşitli yönlerden dezavantajlara sahiptir. Geleneksel yöntemler seçim sistemlerinin gereksinimlerini tam olarak karşılayamamaktadır. Ayrıca toplumsal barışın ve huzurun tesis edilmesi için seçim sistemlerine karşı olan güvenin yüksek olması gerekmektedir.

Gün geçtikçe önemini artıran blockchain teknolojisi, birçok alandaki süreçleri kökünden değiştirecek özelliklere sahiptir. Özellikle finansal alandaki başarılı uygulamalarından dolayı genellikle dijital para ile bağdaştırılmaktadır. Ancak bu teknolojinin sahip olduğu potansiyel bunun çok daha ötesindedir. E-Devlet'ten E-Sağlık'a birçok alanda araştırmacılar çalışmalarına devam etmektedir. Seçim sistemi teknolojilerinin de bu yeni teknolojiden etkilenmemesi düşünülemez. Bu çalışmada, blockchain teknolojisinin sağlamış olduğu faydalardan yararlanılarak, modern ve demokratik kıstaslara uygun bir model sunulmuştur.

Bu tezin ilk bölümünde yaygın olarak kullanılan seçim sistemleri incelenmiş, ardından demokratik ve modern bir seçim sisteminin gereksinimleri ortaya konmuştur. Gereksinimler belirlenirken, çeşitli uluslararası kuruluşların raporları incelenerek, demokratik ve modern bir seçim sisteminin sahip olması gereken kıstaslar göz önüne alınmıştır. Daha sonra ise blockchain teknolojisi ayrıntılı bir şekilde irdelenmiştir. İlk olarak bu teknolojinin bileşenleri ve bu bileşenler arasındaki etkileşim incelenmiştir. Ardından blockchain teknolojisinin mimarisi ve işleyişi incelenmiştir. Teknolojinin uygulama alanları ortaya konulmuştur. Uygulama alanına göre kullanılacak olan blockchain teknolojisinde ne gibi ölçütlerin göz önüne alınması gerektiği saptanmıştır.

İlerleyen bölümlerde ise mevcut seçim teknolojileri ve bunların sahip olduğu sorunlar, ilk bölümde belirlenen gereksinimlere göre ortaya konulmuştur. Ortaya konan sorunları çözecek nitelikte, blockchain tabanlı elektronik seçim modeli oluşturulmuştur. Model oluşturulurken, blockchain teknolojisinin yetersiz kaldığı alanlarda yardımcı modeller kullanılmıştır.

BLOCKCHAIN BASED E-VOTING SYSTEM MODELLING

SUMMARY

Humanity has used elections as a decision-making mechanism since they began to live as a community. Although elections are held in Ancient Greece and Rome, the first modern elections are the choice of representative governments in North America and Europe. With the development of technology, election system technologies have evolved. This process, which started with primitive methods such as marking the votes on palm leaves, is now being carried out with technological methods such as electronic voting machines and remote voting over the internet.

Elections are very critical tools for the proper functioning of democracy. Through elections, citizens transfer their power to those who will represent them. Confidence among the electorate, the state, and the candidates during this power transfer is an indispensable value. The reliability of election systems and the technologies used in these systems play a key role in creating trust among the election stakeholders.

The election process is carried out by institutions of countries in a system by determining the laws and rules. These rules determine the requirements of the electoral system be implemented and set the standards for the whole process. Each institution of a country has its own laws for the electoral processes, which makes it difficult to establish a set of universal election standards. However, when the studies of laws, practices and related institutions are examined, generally agreed and universal election standards can be determined.

Blockchain technology, which increases its importance day by day, has the features that will change the processes in many areas. It is generally associated with digital money because of its successful practices in the financial field. But the potential of this technology is far beyond that. Researchers continue their studies in many fields such as E-Government to E-Health.

Blockchain can be defined as a distributed database type in which transactions are recorded, simply by copying all the computers on the network. In Blockchain, data is stored in fixed structures called blocks. Each transaction must be encrypted before it is added to the end of the chain as a new block, and must be approved by the nodes in the network by the reconciliation mechanism. No centralized mechanism is needed to confirm the operation. It is unthinkable that the election system technologies are not affected by this new technology. In this study, a model suitable for modern and democratic criteria is presented by utilizing the benefits of blockchain technology.

In the first part of this thesis, the electoral systems which are widely used are examined and the requirements of a democratic and modern electoral system have been revealed. In determining the requirements, the reports of various international organizations were examined and the criteria that a democratic and modern electoral system should have been taken into consideration. These criteria can be listed as follows; ensuring that all voters have equal rights of one vote, no voting by proxy or another electorate, the use of secret and unregistered votes, equal accessibility to all voters, voting of an open and transparent method in the counting and processing of votes, voting of election results not being followed in any way until the end of the election process, finding a backup of the votes and re-counting, no change on the ballot papers, being controllable and reliable. Commonly used electoral technologies are paper ballots, lever voting

machines, punched card voting, optical mark-sense voting, direct recording electronic voting, and online voting.

In the following sections, blockchain technology is discussed in detail. First, the components of this technology and the interaction between these components are examined. The main components of blockchain include cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, and blocks. Then, the architecture and the functioning of the blockchain technology were investigated. According to permission models, it is divided into two types, open and private. The consensus methods and the differences in these methods have been revealed. The reasons why soft forks happened and how to solve them were discussed. Then the causes and consequences of hard forks were examined. Smart contracts and the benefits and implementation challenges have been demonstrated. It has been determined what kind of criteria should be taken into consideration in the blockchain technology to be used according to the application area.

In the following section, current election technologies and their problems are presented according to the requirements set out in the first section. The biggest weakness of the paper ballots is the counting of the votes. As in all other vote-counting procedures, the delegation that counts the votes must be representatives of opposing parties, and if a party becomes a majority in this committee, it may affect vote counts in their favor. Lever voting machines do not have any backups of votes. The biggest problem with, punched card voting is that it is not guaranteed to drill a neat hole on the cards. In the optical mark-sense voting, voters must make the marking required by the optical reader manufacturer so that the votes can be read correctly by the optical sensors. Direct recording electronic voting and the biggest concern on online voting is the security problem.

Finally, the blockchain based electronic election model, which will solve the problems, is presented and the advantages and disadvantages of this model are examined. In developing a blockchain based e-election model, election requirements, actors in the election process, the duties and responsibilities of the actors and the performance criteria that the blockchain technology should provide are taken into account. The model consists of three stages: Installation, Voting, Counting of Votes and Announcement of Results. During the installation phase, the regulatory body installs the blockchain network and other systems that will be required. Blockchain records assets such as voter, party and candidate, encryption keys to the network. In the voting process, voters are elected to vote by means of client applications. In this step, the votes are signed in an unknown and secure manner by the blind signature method. Votes, regulatory body and political parties through the network nodes are confirmed and encrypted in the chain is recorded. In the stage of counting of votes and announcement of results, the encrypted votes in the chain shall be resolved in a transparent manner. At this stage, voters can check whether their votes are counted or not. After the counting process is completed, the results are announced.

With the model developed, it was seen that the election requirements mentioned at the beginning of this study were met. However, there are some parts of the model that are open to development. The presented model is very safe due to the advantages of blockchain technology. However, this situation involves the processes after the votes are written to the chain. The security of the client machines in the model is the biggest problem. The backup of the votes is available on all nodes that are joined to the network. Therefore, technically no other backup is needed, but it is unlikely for the

public and stakeholders to fully understand the blockchain technology. In this case, the confidence in the proposed model may be reduced. In order to prevent this, voting papers digitally signed by the voting machines can also be included in the election process. Tens of millions of voters vote in the general elections. This number may also rise to hundreds of millions in some countries. It is important to make sure that the blockchain technology can handle this heavy throughput load.

1. GİRİŞ

Seçim, belirli bir topluluk tarafından oylama yoluyla resmi makamlarda görev yapacakların belirlenmesi, siyasi önerilerin kabul edilmesi veya reddedilmesi biçimidir. Antik Yunan'da ve Roma'da seçimler yapılmasına rağmen, çağdaş dünyadaki seçimlerin kökenleri 17. yüzyıldan başlayarak Avrupa ve Kuzey Amerika'daki temsili hükümetlerin kademeli olarak seçilmesiyle ortaya çıkmaktadır [1].

Seçimler demokrasinin düzgün bir şekilde işleyebilmesi için oldukça kritik araçlardır. Seçimler sayesinde vatandaşlar ellerindeki gücü kendilerini temsil edeceklere aktarırlar. Bu güç aktarımı sırasında seçmenler, devlet ve adaylar arasındaki güven olmazsa olmaz bir değerdir. Seçim sistemlerinin ve bu sistemlerde kullanılan teknolojilerin güvenilirliği, seçim paydaşları arasındaki güveni oluşturmada kilit bir rol oynar. Tarih boyunca seçimler birçok farklı teknoloji kullanılarak yapıldı. Bunlar arasında Hindistan'da Sangam döneminde kullanılan iple bağlanmış ve mühürlenmiş toprak çömleklerden, M.S. 920 yıllarında yine Hindistan'da Çola Hanedanlığınca kullanılan palmiye yapraklarına kadar birçok basit ama etkili araç kullanıldı [2]. Modern dünyada kullanılan yöntemler arasında öne çıkanlar elle sayılan kâğıt oy pusulaları, kollu oy makinaları, delikli kart pusulaları, optik oy pusulaları, doğrudan kayıt eden elektronik oy makinaları ve internet üzerinden oylamadır [3].

Blockchain, sayısız kullanıcı tarafından sürekli güncellenen, bozulması neredeyse imkânsız, ağa dâhil olan ve/veya tüm kullanıcılar tarafından görüntülenebilen, geçmişten günümüze onaylanan tüm işlemlerin tutulduğu, dağıtık dijital bir kayıt defteri olarak düşünülebilir. Hayata geçirilmiş blockchain teknolojisinin ilk sürümü olarak kabul edilebilecek bitcoinden, Satoshi Nakamoto tarafından 31 Ekim 2008 tarihinde, "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" başlıklı bir teknik yazıda bahsedilmiştir [4].

Blockchain teknolojisi getirdiği güvenlik, veri bütünlüğü, genel olarak ve/veya katılımcılar arasında veriye şeffaf bir şekilde erişim sağlanması özelliklerinden dolayı önümüzdeki yıllarda iş ve toplumu etkileyecek önemli teknoloji eğilimlerden biri olarak görülmektedir. Blockchain teknolojisinde, bilgi ağdaki farklı düğümlerde birbirinin kopyası olacak şekilde saklanır ve yeni bilgi sadece düğümler arasında bir mutabakat sağlandığında eklenir. Düğümlerde saklanan bilgi birbiri ardına zincirleme olarak eklenmiş olan veri kümeleri olarak düşünülebilir. Zincir şeklindeki bu veri kümeleri kriptografik zor matematiksel problemlerin bilgisayar gücü ile çözülmesi sonucunda birbirine bağlanmıştır. Bir veri kümesi zincire eklendiğinde, zincirden çıkartılamaz. Blockchain ağının başlangıcından t zamanına kadar olan tüm zincir, ağdaki bütün düğümlerde saklandığından dolayı merkezi bir otoriteye bağımlılık ortadan kalkmaktadır ve ayrıca bu durum hile, sistem hatası, dolandırıcılık gibi riskleri ortadan kaldırmaktadır. Blockchain teknolojisi mülkiyet değişikliği, sertifikalar, lisanslar, hükümet kararları ve mevzuat gibi önemli bilgilerin ve belgelerin depolanması için kullanılabilir. Tipik olarak, zincirde arazi mülkiyeti, doğum ve evlilik sertifikaları, araç sicilleri, eğitim sertifikaları, öğrenci kredileri, sosyal yardımlar ve oylar gibi herhangi bir işleme dayalı veri saklanabilir.

1.1 Konu ve Önemi

Günümüzde bilişim teknolojilerindeki gelişim hayatımızın birçok alanını etkilemektedir. Bunların arasında siyasi karar alma sistemleri olan seçimler de bulunmaktadır. Günümüzde dünyanın çeşitli yerlerinde seçimler elektronik olarak yapılmaya başlanmıştır. Vatandaşların internet üzerinden ulusal kimlik kartlarıyla oylarını kullandığı ülke çapındaki ilk internet seçim sistemi Estonya tarafından kullanılmıştır [5]. Benzer şekilde Norveç 2011 yılında il meclisi seçimlerinde uzaktan elektronik seçim sistemini kullanmıştır [5]. Ancak teknoloji bu noktaya gelmeden önce çok daha ilkel yöntemler kullanıldı. 1858'den önce seçmenler veya siyasi partiler tarafından sağlanan oy pusulaları ile seçimler yapıldı ve hatta birçok yargı üyesi seçiminde oylamalar ses ile yapıldı [3]. Seçimlerdeki bariz hile, standart olmayan oy pusulalarının sayılmasının oluşturduğu zorluk ve maliyet sebebiyle 1888 yılında modern seçim sistemleri Amerika Birleşik Devletlerinde kullanılmaya başlandı [3]. Günümüzde yaygın olarak kullanılan seçim teknolojileri elle sayılan kâğıt oy

pusulaları, kollu oy makinaları, delikli kart pusulaları, optik oy pusulaları, doğrudan kayıt eden elektronik oy makinaları ve internet üzerinden oylamadır [3].

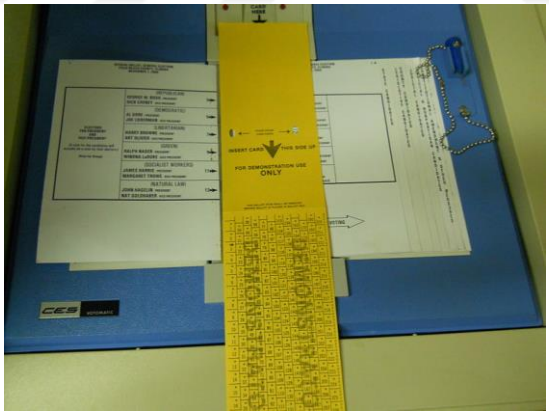
Günümüzde halen birçok ülkede seçimlerde uygulanmakta olan kâğıt oy pusulaları, ilk olarak Avustralya'da, 1858 yılında kullanıldı. Bu seçim yönteminin bilinen diğer adı Avustralya kâğıt oy pusulasıdır. Avustralya kâğıt oy pusulası sisteminde oy pusulaları devlet tarafından standart bir şekilde hazırlanıp, seçmene bir seçim yetkilisi aracılığıyla ulaştırılmakta ve seçmen oyunu gizli bir şekilde pusula üzerinde işaretleyerek, seçim görevlilerinin gözetiminde oy sandığına oyunu atarak işlemi gerçekleştirmektedir [6]. Bu yöntemin en büyük zaafı oyların sayılmasında ortaya çıkmaktadır. Diğer tüm oy sayım işlemlerinde olduğu gibi, oyları sayan heyette karşıt partilerin temsilcileri olmalıdır ve eğer bir parti bu heyette çoğunluk durumuna geçerse oy sayımlarını kendi lehlerinde etkileyebilir [3]. Türkiye Cumhuriyeti 27. Dönem Milletvekili Seçimlerinde kullanılan oy pusulası Şekil 1.1'de görülmektedir [7].

Şekil 1.1 : Türkiye Cumhuriyeti 27. Dönem Milletvekili Seçimi Oy Pusulası.

Mekanik kollu oy makinaları ilk kez 1892 yılında New York'ta kullanıldı. Bu teknoloji, oy sayımının objektif bir şekilde gerçekleştirilebilmesini ve sandıklar kapandıktan sonra oy sayılarının anlık olarak belirlenebilmesini sağlamıştır. Bunların yanı sıra, verilen oyların herhangi bir yedeği tutulmamaktadır. Mekanizmada bir bozulma gerçekleşirse verilen oyları kurtarmak mümkün değildir. Ayrıca bu makinalar binlerce hareketli parçadan oluşmaktadır ve oy verme başlamadan önce sıkı bir şekilde test edilmeleri gerekmektedir [3]. Amerika Birleşik Devletleri seçimlerinde kullanılan kollu oy makinası Şekil 1.2'de görülebilir [8].

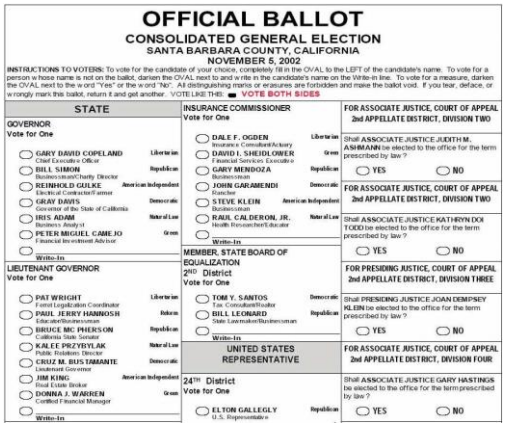
Şekil 1.2 : Kollu Oy Makinası.

Delikli kart pusulaları (Votomatic) ilk olarak 1964 yılında, IBM'in Portapunch delgi mekanizması kullanılarak Georgia'da denendi [3]. Seçmenler seçimlerini belirtmek için önceden tanımlanmış pozisyonlarda, kartlar üzerinde delikler açmaktadır. Bu teknolojinin en büyük sorunu, Votomatic sisteminin kartlar üzerinde muntazam bir delik açmayı garanti edememesidir. 2000 yılındaki Amerika Birleşik Devletleri başkanlık seçiminde, Palm Beach, Florida'da, 433.043 oydan 6.358'inde bu durumla karşılaşılmıştır [3]. Şekil 1.3'te 2000 yılında, Palm Beach'te kullanılan delikli kart pusulası görülebilir [9].



Şekil 1.3 : Delikli Kart Pusulası.

Optik oy pusulalarında, seçmenler oy alanlarını kalemle işaretler ve bu oy pusulaları daha sonra merkezi bir yerde taranır. Oyların optik algılayıcılar tarafından doğru bir şekilde okunabilmesi için, seçmenlerin optik okuyucu üreticisi tarafından istenen işaretlemeyi yapması gerekmektedir. Florida'daki 2000 genel seçimlerinde elde edilen deneysel veriye göre, her 2000 oydan 1'inde yanlış tipte işaretleme yapılmıştır [3]. Optik oy pusulasına bir örnek Şekil 1.4'te görülmektedir [10].



OFFICIAL BALLOT

CONSOLIDATED GENERAL ELECTION

SANTA BARBARA COUNTY, CALIFORNIA

NOVEMBER 5, 2002

INSTRUCTIONS TO VOTERS: To vote for the candidate of your choice, completely fill in the OVAL to the LEFT of the candidate's name. To vote for a person whose name is not on the ballot, darken the OVAL next to and write in the candidate's name on the Write-in line. To vote for a measure, darken the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballot void. If you tear, deface, or wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ● VOTE BOTH SIDES

STATE

GOVERNOR
Vote for One

- GARY DAVID COPELAND — Chief Executive Officer — Libertarian
- BILL SIMON — Business/Charity Director — Republican
- REINHOLD GULKE — Electrical Contractor/Farmer — American Independent
- GRAY DAVIS — Governor of the State of California — Democratic
- IRIS ADAM — Business Analyst — Natural Law
- PETER MIGUEL CAMEJO — Financial Investment Advisor — Green
- Write-In

LIEUTENANT GOVERNOR
Vote for One

- PAT WRIGHT — Forest Legalization Coordinator — Libertarian
- PAUL JERRY HANNOSH — Educator/Businessman — Reform
- BRUCE MC PHERSON — California State Senator — Republican
- KALEE PRZYDYLAK — Public Relations Director — Natural Law
- CRUZ M. BUSTAMANTE — Lieutenant Governor — Democratic
- JIM KING — Real Estate Broker — American Independent
- DONNA J. WARREN — Certified Financial Manager — Green
- Write-In

INSURANCE COMMISSIONER
Vote for One

- DALE F. OGDEN — Insurance Consultant/Actuary — Libertarian
- DAVID I. SHEIDLOWER — Financial Services Executive — Green
- GARY MENDOZA — Businessman — Republican
- JOHN GARAMENDI — Rancher — Democratic
- STEVE KLEIN — Businessman — American Independent
- RAUL CALDERON, JR. — Health Researcher/Educator — Natural Law
- Write-In

MEMBER, STATE BOARD OF EQUALIZATION
2ND District
Vote for One

- TOM Y. SANTOS — Exc. Consultant/Realtor — Democratic
- BILL LEONARD — State Lawmaker/Businessman — Republican
- Write-In

UNITED STATES REPRESENTATIVE
24TH District
Vote for One

- ELTON GALLEGLY — U.S. Representative — Republican

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law?
YES NO

FOR PRESIDING JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION THREE

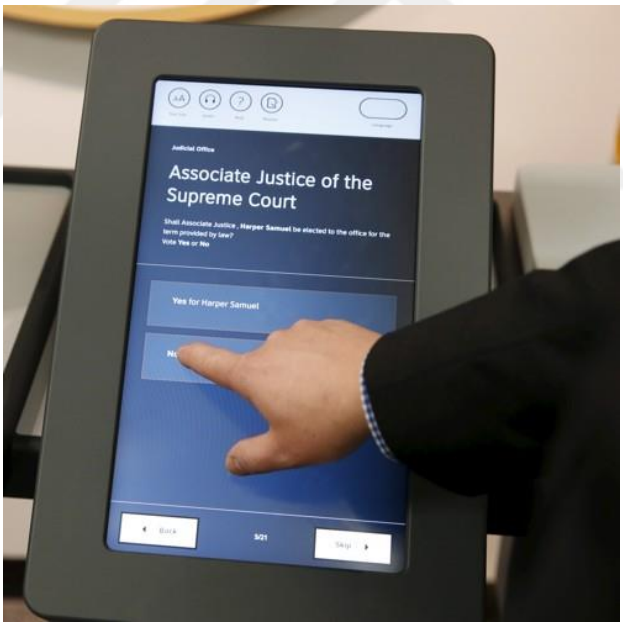
Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION FOUR

Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law?
YES NO

Şekil 1.4 : Optik Oy Pusulası.

Doğrudan kayıt eden elektronik oy makinaları ilk olarak 1974 yılında Amerika Birleşik Devletleri'nde kullanılmıştır. Bu makinalarda, seçmenler adayların yanındaki düğmeye basarak oy verme işlemini gerçekleştirirdi. Günümüzdeki daha modern sürümlerinde ise dokunmatik ekranlar kullanılmaktadır [11]. Şekil 1.5'te bu makinalara bir örnek verilmektedir [12].



Şekil 1.5 : Elektronik Oy Makinası

Internet üzerinden oy kullanımında, seçmenler ağa bağlı herhangi bir bilgisayar üzerinden, kriptolojik olarak güvenliği sağlanan bir protokol ile oy kullanabilmektedir. İnternet üzerinden oy kullanımı ilk olarak 2000 yılında Almanya Osnabruck Üniversitesi'nde ve Arizona, ABD'de gerçekleşti. Bundan beş yıl sonra 2005 yılında, Estonya ülke çapında yerel belediye seçimlerinde internet üzerinden oylamayı kullandı [13].

Günümüzdeki yaygın inanışın aksine, blockchain teknolojisinin arkasındaki temel kavramlar Satoshi Nakamoto'nun makalesinden daha önce 90'lı yıllarda ortaya çıkmıştır. 1991 yılında Stuart Haber ve W. Scott Stornetta tarafından yazılan makalede, belgelerin zaman damgası ile birlikte kripto imzalarla nasıl kullanılacağı anlatılmaktadır [14]. Kaydedilen verilerin silinemeyeceği, merkezi olmayan bir veri depolama sistemi ise Ross Anderson'ın kaleme almış olduğu 1996 yılına ait bir makalede ortaya atılmıştır [15]. Güvenilir olmayan makinalarda saklanan, hassas bilgiler içeren günlük dosyalarının güvenliğinin şifreleme ile nasıl sağlanacağı 1998 yılında Bruce Schneier ve John Kelsey tarafından hazırlanan bir makalede açıklanmaktadır [16]. Blockchain teknolojisinin temellerini oluşturan bu kavramlar, bilgisayar donanımlarındaki yetersizlikten dolayı ortaya atıldıkları tarihte tam olarak uygulamaya geçirilememiştir.

2008 yılında dünya çapındaki ekonomik kriz Lehman Brothers gibi oldukça güvenilir bir firmanın iflasına neden olmuştur. Bu kriz ile birlikte bireylerin kurumlara olan güveni ciddi ölçüde zayıflamış ve iflastan sadece iki ay sonra Satoshi Nakamoto tarafından "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" başlıklı teknik çalışma yayınlanmıştır [4]. Bitcoinin getirmiş olduğu merkezi olmayan ama güvenli, dağıtık, finansal işlem kayıt sistemi krizin yaratmış olduğu kurumlara güvensizlik ortamında oldukça ilgi görmüştür. Ayrıca blokchain teknolojisi ile geliştirilen ilk uygulama olmasından dolayı sonraki yıllarda blockchain ile özdeşleşmiştir. Kullanıcı sayısı ve bilinirliği ile birlikte bakıldığında blockchain teknolojisinin en başarılı uygulaması olduğu söylenebilir.

Bitcoin, kişiler arasında üçüncü bir kuruma/kişiye gerek kalmadan güvenli bir şekilde para transferi yapılmasına olanak sağladı. Bu blockchain teknolojisinin sahip olduğu potansiyelin sadece belirli bir alandaki uygulamasıydı. Bu potansiyelin ortaya çıkarılması Vitalik Buterin tarafından geliştirilen Ethereum platformuyla mümkün oldu. Ethereum ağındaki her bir düğüm Ethereum Sanal Makinası (EVM) adı verilen bir sanal makine çalıştırır. Bu platform, ethereum tarafından sağlanan programlama dilleri ile yazılmış bir uygulamanın çalışmasına olanak sağlamaktadır. Bu programlara akıllı sözleşmeler adı verilmektedir ve bunlar sayesinde blockchain ağı programlanabilmektedir [17]. Bitcoin 1. Nesil blockchain teknolojisi olarak düşünülürken, Ethereum 2. Nesil olarak düşünülmektedir.

1.2 Çalışmanın Amacı ve İçeriği

İnsanoğlu yüzyıllardan beri seçim süreçlerini iyileştirmeye yönelik adımlar atmakta. Yeni bir sistem önerisinde bulunmadan önce, gereksinimlerin neler olduğunun iyi anlaşılması, sistemin daha iyi ve doğru bir şekilde tasarlanması için kilit bir rol oynar. Bu yüzden günümüzde seçim sistemlerinin sağlaması beklenen standartlar ve gereksinimler ele alınarak, tasarım için gerekli olan prensipler belirlenmelidir.

Seçim süreçleri ülkeler veya kurumlar tarafından, kanunlar/kurallar belirlenerek bir sistem içerisinde yürütülmektedir. Bu kurallar uygulanacak olan seçim sisteminin gereksinimleri belirlemekte ve tüm süreç için standartları ortaya koymaktadır. Her ülke veya kurum seçim süreçleri için kendi kanunlarını/kurallarını koymaktadır ve bu durum evrensel bir seçim standartları kümesini oluşturmayı zorlaştırmaktadır. Ancak yasalar, uygulamalar ve ilgili kurumların çalışmaları incelendiğinde üzerinde genel olarak mutabık kalınmış, evrensel nitelikte seçim standartları belirlenebilir.

298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkındaki Kanun'unun ikinci maddesi seçim esaslarını konu almaktadır. Bu maddeye göre;

- Seçimler, serbest, eşit, tek dereceli genel oy esaslarına göre yapılır.
- Seçmen oyunu kendisi kullanır.
- Oy gizli verilir.
- Oyların sayımı, dökümü ve tutanaklara bağlanması açık olarak yapılır. [18]

Bu esaslar uygulanacak olan seçim sisteminin temel gereksinimlerini ortaya koymaktadır. Buna göre seçim sistemi, seçmenlerin baskı altına alınması önleyecek şekilde olmalıdır. Aynı zamanda her seçmenin eşit ve sadece bir oy hakkı olmasını garanti etmelidir. Eşitliğin sağlanabilmesi için oy verme işlemine olan erişilebilirlik en üst seviyede tutulmalıdır. Seçmen oyunu vekâlet yolu ile bir başkasına devredemez. Bir başkası adına oy kullanma ihtimali ortadan kaldırılmalıdır. Oy verme işlemi gizli yapılmalı ve oylar meçhul olmalıdır. Hangi seçmenin kime oy verdiği hiçbir şekilde bilinmemelidir. Oyların sayımı ve kayda geçirilmesi herkese açık ve şeffaf olmalıdır.

2006 yılında Avrupa Hukuk Aracılığıyla Demokrasi Komisyonu tarafından yayımlanan Bağımsız Devletler Topluluğuna Üye Devletlerce Demokratik Seçimler, Seçim Hakları ve Özgürlükler Üzerine Varılan Anlaşmada seçim standartları ve seçim süreçlerine dair gereksinimler belirtilmiştir [19]. Seçim sistemlerini ilgilendiren ve

üzerinde anlaşılan maddeler genel oy hakkı, eşit oy hakkı, gizli oylama, açık ve şeffaf seçimlerdir. Bu maddelere göre; her vatandaşın oy kullanmaya hakkı vardır ve bir oy hakkı veya birbirine eşit ağırlıkta oy hakkı bulunmaktadır. Seçmenler geçersiz oy kullanabilir. Seçmenlerin oy verme işlemine erişilebilirlikleri eşit olmalıdır. Oylar gizli ve hiçbir baskı altında bulunmadan kullanılır. Seçimler açık ve şeffaf olmalıdır.

Seçimler en temelde özgürlük, eşitlik ve gizlilik şartlarını sağlamalıdır. Aynı zamanda, seçim sistemi şeffaf olmalı ve kamu denetimine tabi tutulmalıdır. Birçok ülkenin anayasası genel seçimlerin erişilebilir, özgür, eşit, gizli ve şeffaf olmasını gerektirmektedir. Demokrasinin temel ilkelerini de gözeterek yapısal gereksinimler ve seçim sistemleri prensipleri Çizelge 1.1'de olduğu gibi düşünülebilir [20].

Çizelge 1.1 : Yapısal gereksinimler ve seçim prensipleri.

Yapısal Gereksinimler	**Seçim Sistemi Prensipleri**
Genel Haklar	• Erişilebilirlik • Seçme Hakkı
Özgürlük	• Zorlamaya Maruz Kalmama • Seçim Alanında Propaganda Yapılmaması • Geçersiz Oy Hakkı
Eşitlik	• Adaylar Arası Eşitlik • Seçmenler Arası Eşitlik • Bir Seçmen Bir Oy Hakkı
Gizlilik	• Gizlilik • Gizlilik ve Şeffaflık Arasındaki Denge
Şeffaflık	• Meçhul Oy
Demokrasi	• Güven ve Şeffaflık • Doğrulanabilirdik ve İzlenebilirlik • Güvenilirlik ve Güvenlik • Basitlik

Avrupa Sivil Toplum Örgütleri Kılavuzu Komisyonu tarafından hazırlanan Uluslararası Seçim Standartları kılavuzunda oylama ile ilgili aşağıdaki standartlar ve öneriler belirtilmiştir [21]:

- Tüm oy verme sürecinde ve özellikle oylama sırasında oyların gizliliği sağlanmalıdır.
- Birden fazla oy kullanma ve bir seçmen tarafından bir başkasının oyu üzerindeki herhangi bir kontrolün yasaklanması gerekir.
- Oylama merkezleri engelli seçmenler tarafından erişilebilir ve tasarımları uygun olmalıdır.

Sonuç olarak iyi tasarlanmış bir seçim sisteminin sağlaması gereken şartlar aşağıdaki gibi düşünülebilir:

- Tüm seçmenlerin eşit ve bir oy hakkının garanti altına alınması,
- Vekâleten veya başka bir seçmenin yerine oy kullanılamaması,
- Gizli ve meçhul oy kullanılması,
- Oy verme işlemine erişilebilirliğin tüm seçmenler için eşit olması,
- Oyların sayımı ve işlenmesinde açık ve şeffaf bir yöntemin izlenmesi,
- Seçim sonuçlarının, oy verme işlemi bitene kadar hiçbir şekilde takip edilememesi,
- Oyların yedeğinin bulunması ve yeniden sayımın mümkün olması,
- Oy pusulaları üzerinde herhangi bir değişim yapılamaması,
- Denetlenebilir ve güvenilir olması.

Bu çalışmada yukarıda sayılan tüm gereksinimleri sağlayacak, blokchain tabanlı elektronik bir seçim sistemi önerilecektir. Bu sistem ile geleneksel seçim sistemlerinin sahip olduğu sorunlar ortadan kaldırılacak ve demokrasinin şartlarına uygun bir model ortaya konulacaktır.

2. BLOKZİNCİR (BLOCKCHAİN) BİLEŞENLERİ

Blockchain basitçe ağa katılmış tüm bilgisayarlarda bir kopyası bulunacak şekilde, işlemlerin kaydedildiği, dağıtık bir veri tabanı çeşidi olarak tanımlanabilir. Blockchain'de veri, blok adı verilen sabit yapılarda tutulur [22]. Her bir işlem zincirin sonuna kalıcı olacak şekilde yeni bir blok olarak eklenmeden önce şifrelenmeli ve ağdaki düğümler tarafından mutabakat mekanizmasıyla onaylanmalıdır. Bu işleyişte işlemleri onaylayacak merkezi bir mekanizmaya ihtiyaç duyulmaz [23]. Şekil 3.1'de Blockchain teknolojisinin çalışma akışı görülebilir.

Şekil 2.1 : Blockchain teknolojisinin çalışma akışı.

Bitcoin'in yakalamış olduğu başarıdan sonra birçok insan bitcoin ve blockchain teknolojisine ilgi duymaya başladı. Bu ilgi çoğunlukla kazanç sağlamaya yönelik oldu ve blokchain teknolojisi birçokları tarafından aşırı karmaşık ve anlaşılmaz bulundu. Ancak blockchain teknolojisi hâlihazırda kullanılmakta olan bilgisayar bilimleri, şifreleme ve finans gibi birçok alandaki bileşeni kullanmaktadır. Blockchain'in ana bileşenleri olarak güvenli özetleme fonksiyonları, işlemler, asimetrik anahtar şifreleme, adresler, kayıt defterleri ve bloklar sayılabilir.

2.1 Güvenli Özetleme Fonksiyonları

Güvenli özetleme fonksiyonları blockchain mimarisinin birçok yerinde kullanılmaktadır. Bu fonksiyonlar, matematiksel işlemler kullanarak görece büyük bir veriden daha küçük ve nispeten benzersiz bir veri, diğer bir deyişle özet, çıkarmak üzere tasarlanır. Bu özet değerler aynı girdi için aynı çıktıyı üretirler ancak girdideki ufak bir değişiklik bile çok daha farklı bir çıktı üretmek için yeterlidir. Aynı zamanda üretilen çıktı değerleri sabit uzunlukta olurlar. Güvenli özetleme fonksiyonlarının taşıması gereken özelikler aşağıdaki gibidir:

- Verilen girdi mesajı için çıktı özeti hızlı bir şekilde bulunmalıdır.
- Tek yönlüdürler, yani verilen bir çıktı değeri için girdi değerini hesaplamak imkânsıza yakındır. Öyle ki, özet çıktıdan girdiye ulaşmanın tek yolu, girdi kümesindeki her olası mesaj için güvenli özetleme fonksiyonunu çalıştırıp, oluşan çıktı ile elimizdeki özet bilgiyi karşılaştırmaktır. Örneğin verilen y özet değeri için öyle bir x değeri bulalım ki $hash(x) = y$ olsun.
- Verilen iki farklı girdi için aynı çıktıyı üretecek değerleri bulmak hesaplama süresi bakımında imkânsızdır. Örneğin, verilen x değeri için öyle farklı bir y değeri bulalım ki $hash(x) = hash(y)$ olsun.

MD5, SHA-1, SHA-2 gibi birçok özetleme fonksiyonu olmasına rağmen çoğu blockchain uygulamasında SHA-256 özetleme fonksiyonu kullanılmaktadır. Birçok bilgisayar bu fonksiyonu donanım seviyesinde yürütebilmektedir ve bu durumdan dolayı hesaplanması daha hızlı olmaktadır [24].

SHA-256 algoritması 256 bitlik uzunluğa sahip özet çıktılar üretmektedir, bu da 2^{256} tane olası çıktı anlamına gelmektedir. Çıktı sayısı sonlu bir küme olduğundan teorik olarak iki farklı girdinin aynı çıktı değerine sahip olması ya da bir başka deyişle özet bilgilerin çakışması mümkündür. Ancak 2^{256} yaklaşık olarak 10^{77} yapmaktadır ve gözlemlenebilir evrendeki atom sayısının 10^{80} civarında olduğu düşünülürse bu ihtimal imkânsıza yakındır [25]. SHA-256 özetleme fonksiyonunda bir çakışma bulabilmek için ortalama olarak 2^{128} kere yürütmek gerekir, bu da yaklaşık olarak $3{,}402 \times 10^{38}$ etmektedir. Bu ihtimali daha iyi anlamak için Bitcoin ağının 2015 yılındaki özetleme oranı (hash rate), saniyede çıkarılan özet sayısı (hashes per second), olan 300 katrilyon referans olarak düşünülebilir. Bu hızda bile tüm ağın bir çakışma üretmesi yaklaşık olarak $3{,}6 \times 10^{13}$ yıl sürecektir ki evrenin yaklaşık olarak hesaplanan yaşı $1{,}37 \times 10^{10}$ yıldır [26]. Çizelge 2.1'de SHA-256 özetleme algoritmasına göre örnek girdi ve çıktı değerleri görülebilir.

Çizelge 2.1 : SHA-256 Algoritmasına göre örnek girdi ve çıktı değerleri.

Örnek mesaj (girdi) değeri	**Çıktı (özet) değeri**
B	DF7E70E5021544F4834BBEE64A9E3789FEBC4BE81470DF629CAD6DDB03320A5C
Blockchain	625DA44E4EAF58D61CF048D168AA6F5E492DEA166D8BB54EC06C30DE07DB57E1
blockchain	EF7797E13D3A75526946A3BCF00DAEC9FC9C9C4D51DDC7CC5DF888F74DD434D1
Blockchain basitçe dağıtık bir veri tabanı çeşidi olarak tanımlanabilir.	F37059658DCF143D874B61CF29F57EF80E2DA6BC518973615471CB542690D478
Okunabilirlik açısından 16'lık sayı düzeninde gösterilmiştir.	

2.1.1 Tek seferlik şifreleme anahtarı (cryptographic nonce)

Bu yöntemle rasgele üretilen bir anahtar, özetlenecek veriyle birleştirilerek farklı çıktılar elde etmek için kullanılır. Sadece anahtar değeri değiştirilerek aynı ham veri için farklı özet değerleri elde edilebilir.

$$Hash(veri + anahtar) = \text{özet}$$

2.2 İşlemler

İşlem, taraflar arasındaki etkileşim olarak tanımlanabilir. Blokchain ağlarında ise, taraflar arasındaki dijital varlık transferi olarak görülebilir. Ağdaki her bir blok bir veya daha fazla sayıda işlem içerebilir. Bazı blockchain ağlarında güvenlik amacıyla hiç işlem içermeyen bloklarda bulunabilir. Bu sayede kötü niyetli bir düğümün, daha uzun ve değiştirilmiş bir zincir elde etmesi engellenir.

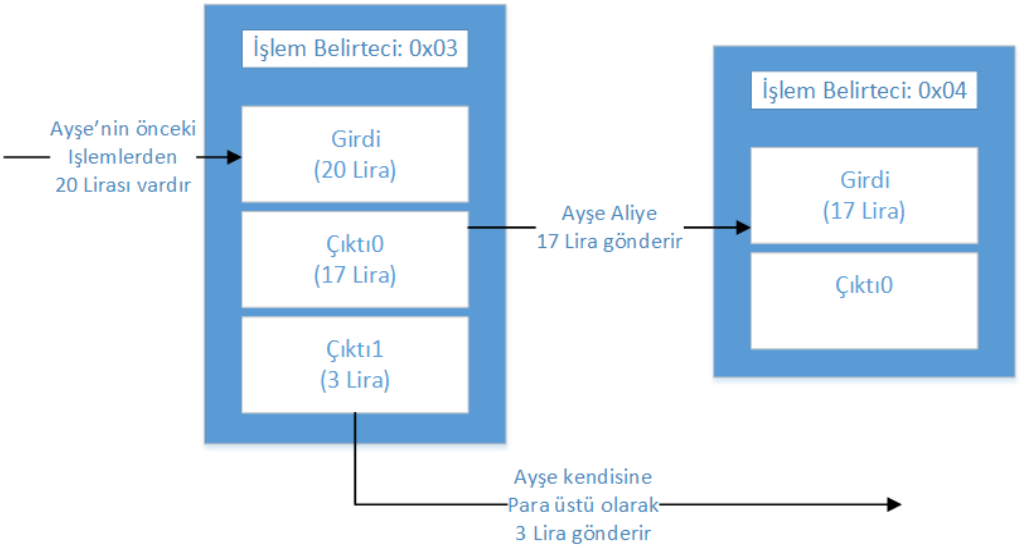
Her Blockhain ağındaki işlem süreçleri farklı olsa da kabaca aynı adımları içermektedir. Bir kullanıcı blockchain ağına gönderici adresi, göndericinin açık anahtarı, dijital bir imza işlem, girdisi ve çıktısından oluşan istek gönderir. Ağa gönderilen işlemde, daha fazla olabileceği gibi, genel olarak bulunan bilgiler ikeye ayrılır:

2.2.1 Girdiler

Aktarılacak dijital varlıkların bir listesidir. İşlem kendisinden önceki işleme bir referans içerir ve işlemin girdisi kendisinden önceki işlemlere referans verdiğinden, dijital varlıklar değişmez. Bunun yerine dijital varlıklar bölünebilir veya birleştirilebilir. Bölünme veya birleşme işleminde varlıkların toplam değerleri de korunmaktadır. Bu durum özellikle bitcoin gibi kripto paralarda daha anlaşılır olmaktadır. Varlıkların bölünmesi veya birleştirilmesi işlem çıktılarında belirtilir. Ayrıca göndericinin belirtilen girdilere erişimi olduğunu kanıtlaması gerekir. Bunu da genellikle işlemi dijital olarak imzalayarak yapar. Bu sayede özel anahtara erişimini kanıtlamış olur.

2.2.2 Çıktılar

Çıktılar genel olarak alıcıların ne kadar dijital varlığa sahip olacağını belirten hesaplardır. Her bir çıktı, alıcılara aktarılacak varlıkları, alıcıların tanımlayıcılarını (id, adres) ve alıcıların bu değerleri kullanmak için yerine getirmesi gereken koşulları belirler. Ayrıca gönderilen dijital varlıklar gereğinden fazla ise, fazlalık göndericiye geri gönderilir (para üstü) [27]. Örnek işlem girdi ve çıktıları Şekil 3.2'de gösterilmektedir.

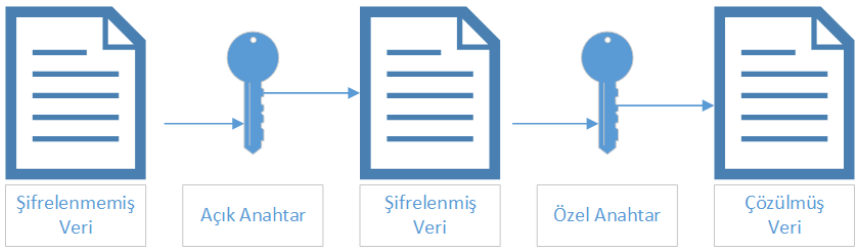


Şekil 2.2 : Örnek işlem girdi ve çıktısı.

Blockchain dijital varlıkların transferi dışında veri aktarımı için de kullanılabilir. Örneğin, verilmiş bir oyun değeri herkes tarafından görülebilecek (gizli oy ve meçhul oy gereksinimleri sağlanarak) ve değiştirilemeyecek şekilde zincire eklenebilir.

2.3 Asimetrik Anahtar Şifreleme

Bu yöntemde biri açık (public) diğeri özel (private) olmak üzere iki anahtar kullanılır. Bu yöntem aynı zamanda açık anahtar şifrelemesi (Public Key Encryption) olarak da adlandırılır. Açık anahtar, herkes tarafından bilinebilir ancak şifrelenen verinin güvenliği için özel anahtarın gizliliği esastır. Bu iki anahtar matematiksel olarak birbiriyle bağlantılıdır ve teorik olarak açık anahtardan özel anahtar elde edilebilir ancak bunun gerektirdiği çok yüksek hesap gücünden dolayı imkânsız olarak görülmektedir. Bir mesaj özel anahtar ile şifrelenirse sadece açık anahtar ile çözülebilir, aynı şekilde açık anahtar ile şifrelenirse yalnızca özel anahtar ile çözülebilmektedir. Şekil 3.3 özel ve açık anahtar çiftinin asimetrik şifrelemede nasıl kullanıldığını göstermektedir.



Şekil 2.3 : Asimetrik şifreleme.

Bu yöntemde veriler herkes tarafından ulaşılabilir olurken, verilerin bütünlüğü ve kaynağının doğruluğu sağlanmış olur. Bu sayede birbirini tanımayan kullanıcılar arasında güven ilişkisi sağlanır. Blockchain ağında bunu yapmak için işlemler dijital olarak imzalanır yani özel anahtar ile şifrelenir ve açık anahtara sahip herkes tarafında bu şifre çözülebilir. Açık anahtar herkesin kullanımına açık olduğundan, özel anahtar ile şifrelenmiş işlem, işlemi imzalayanın özel anahtara erişimi olduğunu kanıtlamaktadır. Açık anahtarlı şifrelemenin en büyük dezavantajı yavaş çalışmasıdır.

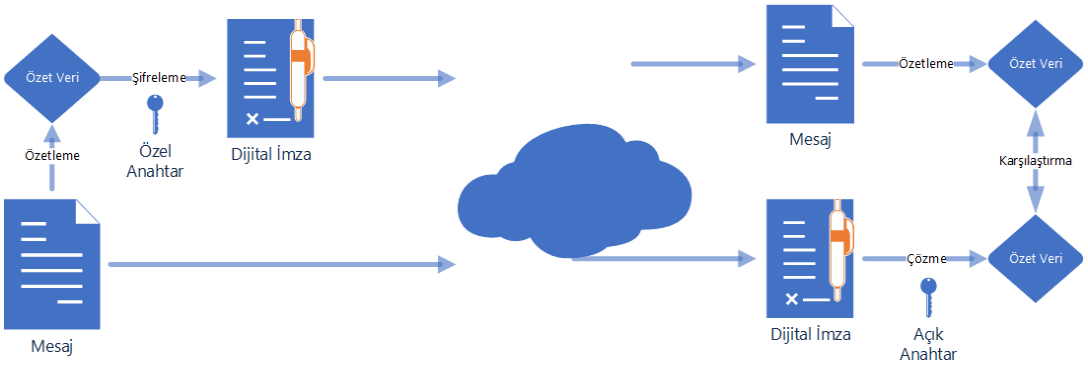
Bir diğer şifreleme yöntemi ise simetrik şifrelemedir (Symmetric Encryption). Bu yöntemde hem şifreleme, hem de çözümlemede aynı anahtarlar kullanılmaktadır. Şifrelenen verinin güvenliği için anahtar bilgisi sadece ilgili taraflar arasında paylaşılmalıdır. Simetrik şifreleme açık anahtar şifrelemeye göre çok daha hızlı çalışmaktadır. Bundan dolayı, aktarılacak verinin kendisi değil, simetrik şifrelemede kullanılacak anahtar bilgisi açık anahtar şifreleme ile şifrelenir. Veri ise simetrik şifreleme kullanılarak şifrelenir ve bu sayede hızlanma sağlanmış olur.

Blockchain ağlarında kullanılan dijital imzalama adımları aşağıdaki gibidir.

Ali'nin Ayşe'ye veri aktaracağını düşünelim:

- Ali, Ayşe ile açık anahtarını paylaşır.
- Ali, Ayşe'ye göndereceği mesajın, SHA-256 gibi bir güvenli özetleme algoritmasıyla özetini çıkarır.
- Ali özet değerini özel anahtarı ile şifreleyip mesaja ekler.
- Ali mesajı Ayşe'ye gönderir.
- Ayşe mesajı aldığında mesajın özet değerini oluşturur ve Ali'nin eklemiş olduğu şifreli özet bilgisini Ali'nin açık anahtarı ile çözer. Eğer her iki özet bilgisi aynı değilse;
    - Mesajı imzalayan kişi Ali değildir veya
    - Mesaj içeriği değiştirilmiştir.

Şekil 3.4 dijital imza akışını göstermektedir.



Şekil 2.4 : Dijital imza akışı.

Asimetrik anahtar şifreleme blockchain ağlarında genellikle aşağıdaki sebeplerden kullanılır:

- Özel anahtarlar işlemleri dijital olarak imzalamak için,
- Açık anahtarlar adresleri üretmek için,
- Açık anahtarlar, özel anahtarlar ile üretilen imzaları doğrulamak için [28]

2.4 Adresler

Blockchain uygulamalarında adresler genel olarak bir işlemin nereden nereye yapılacağını belirtmek için kullanılır. Çoğu ağda, kullanıcının açık anahtarına sürüm numarası, sağlama toplamı gibi ek alanlar eklenir ve bu veri güvenli özetleme fonksiyonlarına girdi olarak verilerek adres değeri oluşturulur. Adresler açık anahtarlardan daha kısadır.

Blockchain ağ kullanıcıları, ağdaki tek adres kaynağı olmayabilir. Bir akıllı sözleşme ağa dağıtıldıktan sonra, bu sözleşmeye erişilebilirlik gerekir. Örneğin Ethereum ağında, akıllı sözleşmelere sözleşme hesabı adı verilen özel bir adres ile ulaşılır [29].

2.4.1 Cüzdanlar

Blockchain ağındaki kullanıcıların özel anahtarları büyük bir öneme sahiptir. Bir kullanıcı özel anahtarını kaybederse, o anahtarla ilişkilendirilmiş tüm dijital varlıklar kaybolur, çünkü aynı özel anahtarı yeniden oluşturmak hesaplama gücü bakımından imkânsızdır. Kullanıcılar özel anahtarlarını genellikle cüzdan adı verilen özel yazılımlarda saklarlar. Cüzdanların özel anahtarları saklamak dışında dijital varlıkların değerini hesaplamak gibi başka işlevleri de vardır.

Bir kullanıcıya ait özel anahtarların kötü niyetli kişilerce ele geçirilmesi geri döndürülemeyecek ciddi sonuçlar doğurabilir. Blockchain ağındaki verilerin değiştirilememesinden dolayı, özel anahtarları ele geçiren bir suçlu bu anahtarlara ait dijital varlıkları başka bir hesaba transfer ettiğinde, bu işlem geri alınamaz [29].

2.5 Kayıt Defterleri

Bir kayıt defteri, o güne kadar olan tüm işlemlerin tutulduğu bir veri tabanı olarak düşünülebilir. Modern zamanlarda kayıt defterleri genellikle dijital olarak, güvenilir, merkezi bir taraf tarafından saklanmaktadır. Blockchain teknolojisi ise kayıt defterlerinin dağıtık bir mimaride, güvenli bir şekilde saklanmasına olanak sağlamıştır. Dağıtık mimaride saklanan kayıt defterlerinin, merkezi yapıda saklananlara göre birçok avantajı bulunmaktadır [30]. Çizelge 2.2'de merkezi ve dağıtık blockchain mimarisindeki kayıt defterlerinin karşılaştırılması yapılmıştır.

Çizelge 2.2 : Merkezi ve Dağıtık Blokchain Mimarisinde Cüzdanlar

Merkezi Mimari	**Dağıtık Blockchain Mimarisi**
Merkezi mimaride saklanan defterler kaybolabilir veya yok olabilir. Kullanıcılar, merkezin sistemi düzgün bir şekilde yedeklediğine güvenmelidir.	Blockchain ağında, defterler tüm düğümlere dağıtılır ve senkronize edilir. Her düğümde defterin bir kopyası bulunur ve bundan dolayı defterin tamamen yok edilmesi oldukça zorlaşır.
Merkezi defterler tüm ağ, donanım, yazılım altyapısının aynı olduğu homojen bir ortamda saklanabilir. Bu durumda, ağın herhangi bir yerindeki saldırı, ağın geri kalanında da çalışacağından tüm sistemin dayanıklılığı etkilenir.	Blockchain ağları heterojen yapıdadır. Bu yüzden ağın herhangi bir yerinde çalışan bir saldırının, tüm ağda aynı etkiyi göstermesi beklenmez.
Merkezi defterler, belirli bir coğrafik konumda bulunabilir. Bu konumda meydana gelen kesintilerde deftere erişim veya ona bağlı hizmetlere erişim kesintiye uğrayabilir.	Blockchain ağındaki düğümler coğrafi olarak birbirinden farklı konumlarda bulunur. Bu yüzden yerel oluşabilecek kesintilerden ağın tamamı etkilenmez.

Çizelge 2.3 (devam): Merkezi ve Dağıtık Blokchain Mimarisinde Cüzdanlar

Merkezi Mimari	**Dağıtık Blockchain Mimarisi**
Merkezi defterlere işlem kaydetme şeffaf bir şekilde gerçekleşmez. Kullanıcılar, işlemlerin geçerliliği konusunda merkezi otoriteye güvenmek zorundadır.	Blockchain ağında, tüm işlemlerin doğruluğu ve geçerliliği kontrol edilir. Kötü niyetli bir düğüm geçersiz bir işlem eklemeye çalıştığında ağdaki diğer düğümler bu işlemi reddeder ve zincirin geçerliliği korunur.
Merkezi defterlerdeki işlem listesinin bütünlüğü garanti edilemez. Kullanıcılar, merkezi otoritenin tüm geçerli işlemleri kaydettiğine güvenmek zorundadır.	Blockchain ağında, tüm geçerli işlemler düğümlere dağıtılmış bir şekilde tutulur. Zincire yeni bir blok eklenirken önceki bloğa referans verilmesi gerekir. Bu yüzden yeni eklenecek blok bir önceki bloğa referans vermezse diğer düğümler tarafından reddedilir ve veri bütünlüğü sağlanmış olur.
Merkezi defterde geçmişe yönelik kayıtlar değiştirilebilir. Kullanıcılar merkezi otoritenin geçmişteki kayıtları değiştirmediğine güvenmek zorundadır.	Blockchain ağında, geçmişe yönelik değişikliği engellemek için güvenli özetleme fonksiyonları ve dijital imzalar gibi yöntemler kullanılır.

2.6 Bloklar

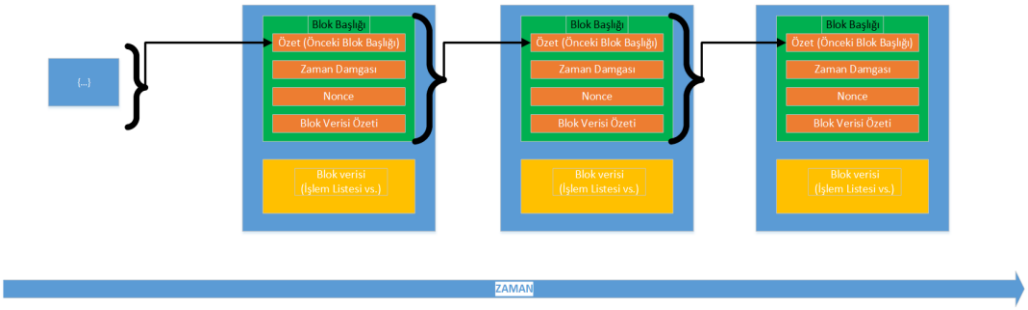
Blockchain ağında, kullanıcılar istemci yazılımlar aracılığıyla ağdaki bir veya birkaç düğüme işlemler gönderir. Bu işlemler ardından ağdaki diğer düğümlere dağıtılır. Ağa dağıtılan bu işlemler doğrulanıp, onaylanana kadar bir kuyrukta bekletilir. Ancak yayımcı bir düğüm tarafından yayınlandığında zincire eklenir.

Bir blok, başlık ve blok gövdesinden oluşur [23]. Başlıkta bu blok için meta veriler bulunmaktadır. Gövdesinde ise onaylanmış ve güvenilir işlemlerin bir listesi bulunur. Onaylama ve güvenilirlik bloğun doğru formatlanmasından ve blok içeriğindeki her bir işlemin güvenli bir dijital imzaya sahip olmasından anlaşılır. Dijital imza, dijital varlık sahiplerinin, bu imzayı oluşturabilecek özel anahtara sahip olduklarını kanıtlar. Diğer düğümler yayınlanan bloktaki tüm işlemlerin geçerliliğini ve doğruluğunu

kontrol ederek, geçersiz işlem içeren blokları reddederler. Birçok blockchain uygulamasında kullanılan veri alanları aşağıdaki gibidir:

- Blok Başlığı
    - Bazı blockchain ağlarında blok yüksekliği olarak da bilinen blok numarası.
    - Önceki blok başlığın özet değeri.
    - Blok verisinin özeti (Merkle Ağacı).
    - Zaman damgası.
    - Bloğun büyüklüğü.
    - Tek seferlik şifreleme anahtarı (nonce value). Madenciliği kullanan blockchain ağlarında, özet bulmacasını çözmek için, yayıncı düğüm tarafından kontrol edilen değer.
- Blok Gövdesi
    - İşlemler listesi.

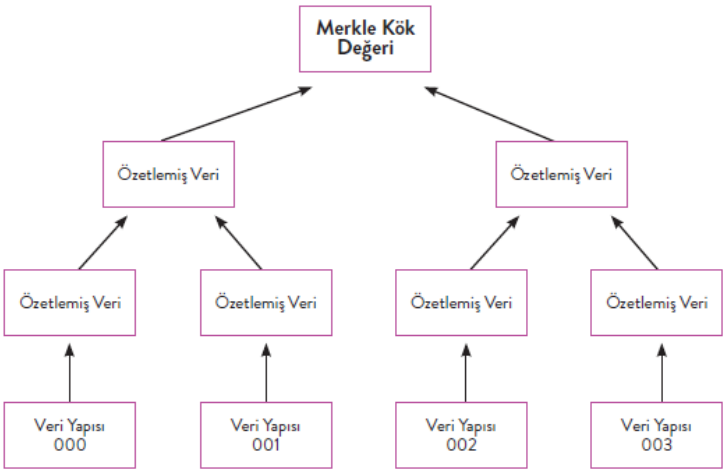
Her bir blok, kendisinden önceki bloğun başlığındaki özeti içerecek şekilde zincirlenir. Daha önce yayınlanan bir blok değiştirildiğinde özet bilgisinin de farklı olması beklenir. Bu durum zincirleme olarak kendisinden sonraki bloklarda da görülür, çünkü her blok kendisinden önceki bloğun özetinin içermektedir. Bu durum değiştirilen blokların belirlenmesini ve zincirden çıkarılmasını kolaylaştırır [31]. Şekil 2.5'de örnek blok yapısı görülebilir.



Şekil 2.5 : Örnek blok yapısı.

2.6.1 Merkle ağacı

Tüm veriyi temsil edecek şekilde, verinin tekil bir kök özeti olana kadar karıştırıldığı ve birleştirildiği bir veri yapısıdır. Blok verisinin özeti bu şekilde çıkarılır. Büyük veri kümelerinin hızlı ve güvenli bir şekilde özetinin çıkartmakta ve doğrulamada kullanılır. Bu veri yapısı ikili bir ağaç yapısından oluşur. Bu ağacın dallarında verinin parçaları bulunur. Daha sonra köke doğru özet bilgi çıkarılarak birleştirilir ve en son tekil kök değeri elde edilir [32]. Şekil 2.6'da merkle ağaç yapısı gösterilmiştir.



Şekil 2.6 : Merkle ağaç yapısı.

3. BLOCKCHAİN MİMARİSİ VE İŞLEYİŞİ

Blockchain mimarisinde merkezi bir yapı bulunmamaktadır. Ağın bakımını ve sürekliliğini, ağa katılan kullanıcılar üstlenmektedir. Ağa katılan her kullanıcıya düğüm adı verilir. Düğümler zincire eklenecek yeni blokların üretilmesinden, doğrulanmasından ve onaylanmasından sorumludur. Bloklara hangi işlemlerin ekleneceğini veya eklenmeyeceğini, eklenecek işlemlerin öncelik sıralarını belirlerler. Düğümler ikiye ayrılmaktadır; tam düğümler, aynı zamanda yayımcı düğümler olarak da bilinirler ve hafif düğümler. Yayımcı düğümler, zincirin tamamının bir kopyalarını tutarlar ve işlemlerin geçerliliğini test ederler. Aynı zamanda zincire yeni blok eklenmesinden ve zincirin bakımından da yayımcı düğümler sorumludur. Hafif düğümler ise zincirin bir kopyasını tutmazlar ve işlemlerini yayımcı düğümlere aktarmakla sorumludurlar.

Zincire yeni eklenecek bloklarda işlemlerin verisi bulunmaktadır. Ağa dâhil olan düğümler yeni işlemler oluşturabilirler. Bu işlemler bir havuzda kuyruklanır. Her yayımcı düğüm bir sonraki bloğu üretmeye aday olabilir ve blokları üretirken havuzdaki işlemlerden bir veya birkaçını seçebilir. Bu seçme işlemi sırasında, işlemin yaratılma tarihi ve işlem için ödenmiş masraf hangi işlemlerin daha önce bloğa ekleneceğine karar vermek için kullanılır. Örneğin, bitcoin ağında masraf değeri çok düşük olduğundan ortalama bekleme süresinin aşmış çokça işlem bulunmaktadır.

Bloklar oluşturulurken tüm özet (hash) değerleri blok yapısına uygun şekilde oluşturur. Sonrasında bloğa eklenmiş işlemlerin sahipliği dijital imza ile kontrol edilerek doğrulanır. Bu blok tüm yayımcı düğümler arasında yayılarak kontrol edilir. Bu kontrol sırasında diğer yayımcı düğümler bu blokların yapısını ve içeriğini kontrol ederler. Uygun bulunmayan bloklar reddedilir. Blockchain ağında merkezi bir otorite bulunmadığından, yeni eklenecek bloğun hangi düğüm tarafından yaratılacağı zor kriptografik bulmacaların çözümüyle belirlenir. Düğümler çözüm için tek seferlik rastgele bir değeri (nonce) tahmin etmeye çalışırlar ve bunun için yüksek miktarda bilgisayar gücü harcanır. Bu bilgisayar gücü yüksek miktarda elektrik gücü

istemektedir. Bu masrafın gönüllü bir şekilde karşılanması mümkün değildir. Bu yüzden çözümü bulan düğüm ödüllendirilir ve bu sayede sisteme yeni düğüm eklenmesi ve mevcut düğümlerin korunması sağlanır. Aynı zamanda işlemler için ödenmiş masraflarda düğümler tarafından harcanan işlem gücü masrafını karşılamak için kullanılır. Zincire yeni eklenen bu blok tüm ağda yayınlanır ve diğer düğümlerde kendilerinde bulunan zincirin kopyasına bu düğümü eklerler. Düğümler arasındaki, blokların kontrol edilmesi ve zincire eklenmesi işlemine uzlaşma adı verilir. Farklı blockhain ağlarındaki uzlaşma yöntemleri ilerleyen kısımlarda ayrıntılı şekilde ele alınacaktır.

3.1 Blockchain Türleri

Blockchain ağları, izin modellerine göre türlerine ayrılabilirler. Herkesin erişimine açık olan blockchain ağları açık ağlar olarak adlandırılabilir. Ağa erişimin, belirli bir grup ya da bir organizasyon tarafından belirlenmesinde özel bir ağdan bahsedilebilir [33].

3.1.1 Açık ağlar

Açık ağlar mutabakat yapısına katılımın izin gerektirip gerektirmemesine göre "Tamamıyla İzin Gerektirmeyen Blockhain Ağları" ve "Kısmen İzin Gerektiren Blockchain Ağları" olarak ikiye ayrılabilir. Açık ağlarda, herhangi bir izin mekanizması gerekmediğinden kötü niyetli düğümler ağa kolayca katılabilir. Bu tip ağlarda, zincirin kötü niyetli düğümler tarafından bozulmaması için yüksek işlemci gücü gerektiren mutabakat yöntemleri kullanılır. Bu yüksek işlemci gücüne rağmen ağa katılımı arttırmak için ödül sistemleri uygulanmaktadır.

3.1.1.1 Tamamıyla izin gerektirmeyen blockhain ağları

Ağa katılarak kayıtları okumak için ve mutabakat yapısına dâhil olarak zincire yeni düğümler eklemek için herhangi bir izin gerekmiyorsa, bu tür blockchain ağlarına "Tamamıyla İzin Gerektirmeyen Blockhain Ağları" denir. Bu türdeki ağlarda olabildiğince çok düğümün ağa dâhil olarak, mutabakat sürecinde rol almasıdır. Bu sayede ağın ve zincirin güvenliği artacaktır. Ancak bu tür ağlarda düğümlerin ağa dâhil olması için bir çıkarı olmalıdır. Bu da zincire yeni blok ekleyen düğüme verilecek olan ödülle çözülebilir. Bu ağlara en bilenen örnek bitcoindir.

3.1.1.2 Kısmen izin gerektirmeyen blockchain ağları

Kısmen izin gerektirmeyen blockchain ağlarında, kayıtlı verileri yani zinciri okuma için herhangi bir izin gerekmez ancak ağa dâhil olup mutabakat yapısına uyarak zincire yeni bloklar eklemek için belirli bir kurumun veya organizasyonun izni gerekmektedir. Buna örnek olarak, akademik dünyada yayınlanan makalelerin tutulacağı bir blockchain ağı verilebilir. Bu hayali ağda seçilmiş ve izin verilmiş düğümler, yayımlanmak istenen makalenin gerçekliğini ve makalede intihal oranını belirleyerek, mutabık kalınan koşullara uyuyorsa, makaleyi zincire ekleyebilir. Bu zincirdeki makaleler ise herhangi bir izin gerektirmeden tüm dünyanın kullanımına açılabilir.

3.1.2 Özel ağlar

Açık ağlarda veriye herkes tarafından erişilebilir. Şirketler, organizasyonlar ve kamu kurumları gibi kuruluşlar açık ağlar üzerinde veri bulundurmayı tercih etmeyebilirler. Her ne kadar veriler şifrelenmiş bir biçimde bulunsa da şifreler kırılabilir ve veriler kötü niyetli kişiler tarafından sızdırılabilir. Bu durumda özel blockchain ağları ile veriye erişim kısıtlanır ve sadece yetki verilmiş düğümler tarafından sağlanabilir.

3.1.2.1 Kısmen izin gerektiren blockchain ağlar

Kısmen izin gerektiren blockchain ağları, ağdaki veriye erişim ve okuma için izin gerektiren ancak ağa katıldıktan sonra mutabakat süreçlerine dâhil olarak zincire yeni bloklar eklemek için izin gerektirmeyen ağlardır. Bu sayede ağ katılımcıları arasında güvenli bir veri kayıt sistemi oluşturulabilir. Buna örnek olarak, devlet kurumları arasında güvenli bilgi alışverişini sağlayacak bir ağ örnek verilebilir. Ağa katılan kurumlar, ağdaki verilere erişebilir ve yeni veriler ekleyebilir. Böylece bir kurumda gerçekleşebilecek bir arıza durumunda veri kaybı yaşanmayacak ve diğer kurumlar işleyişlerine devam edebilecektir.

3.1.3 Bütünüyle izin gerektiren blockchain ağları

Bu tip ağlarda, ağa katılarak veriye erişim ve mutabakat sistemine katılarak zincire yeni veri ekleme ayrı ayrı izin gerektirir. Çizelge 3.1'de blockchain ağ türlerinin karşılaştırılması görülebilir [33].

Çizelge 3.1 : Blockchain ağ türlerinin kaşılaştırılması.

Özellik	Açık Ağlar	Özel Ağlar
Mutabakat Yöntemine Dâhil Olan Düğümler	İzin Gerektirmiyor / Tüm Yayımcı Düğümler	İzin Gerektiriyor / Seçili Yayımcı Düğümler
Okuma İzni	Açık	Kısıtlı
Verinin Değişmezliği	Neredeyse İmkânsız	Değiştirilebilir
Verimlilik	Düşük	Yüksek
Merkezlilik	Dağıtık	Merkezi

3.2 Uzlaşma (Mutabakat) Yöntemleri

Blockchain ağlarında, düğümler arasında uzlaşmaya varmak Bizans Generalleri problemine benzemektedir. Bu problemde, bir grup general bir şehri çevrelemiştir. Aralarından bazıları saldırmayı düşünürken, geri kalanları geri çekilmeyi düşünmektedir. Saldırı sadece topyekûn bir şekilde gerçekleştirilirse başarılı olabilmektedir. Bu durumda, arazide dağıtık bir şekilde konuşlanmış generallerin anlaşmaya varması gerekmektedir [33].

Hangi düğümün, zincire eklenecek bir sonraki bloğu yayınlayacağı ve aralarında anlaşmaya varması blockchain teknolojisinin anahtar süreçlerinden birisidir. Bu problem, ağa katılan düğümlerce kabul edilen mutabakat yöntemleri ile çözülmektedir. Açık ağlarda, bir sonraki bloğu yayınlamak için birbiriyle yarışan birçok düğüm vardır. Bu yarış oldukça rekabetçidir çünkü kazanan düğüm ödül veya işlem ücretleriyle finansal kazanç elde eder.

Bir düğüm, blockchain ağına katıldığında sistemin başlangıç bloğunu yani genesis adı verilen ilk bloğu şartsız şekilde kabul eder. Her zincir genesis bloğu ile başlamaktadır. Zincire eklenen bloklar birbiri ardına mutabakat yöntemine göre onaylanarak eklenmektedir. Bununla birlikte, mutabakat yönteminde bağımsız olarak, her bir blok geçerli olmalı ve her düğüm kendi başına tüm zinciri doğrulayabilmelidir. Böylece düğümler genesis bloğu ve ondan sonra gelen blokları ekleyerek tüm zincir bağımsız bir şekilde doğrulayabilir. Mutabakat yöntemleri aşağıdaki özellikleri içermelidir [34]:

- Genesis blok üzerinde anlaşılmıştır.
- Kullanıcılar hangi blokların zincire ekleneceğine dair mutabakat yöntemi üzerinde anlaşmıştır.

- Her bir blok, kendinden önceki bloğun başlık özet değerinin içermektedir ve bu sayede kendinden önceki bloğa bağlanmış olur. (Genesis blok istisna olarak düşünülebilir.)
- Her bir kullanıcı zinciri bağımsız olarak doğrulayabilir.

3.2.1 İşin ispatı (proof of work) uzlaşma yöntemi

İşin ispatı modelinde, yüksek hesaplama gücü gerektiren matematiksel bir modeli ilk çözen kişi bir sonraki bloğu yayınlama hakkı elde eder. Bulmacanın çözümü yapılan işin kanıtı niteliğindedir. Bulmaca, çözümün zor olacağı ancak geçerliliğinin kolaylıkla kontrol edileceği şekilde tasarlanır. Bu sayede diğer düğümler çözümü kolayca onaylar ve yeni blok zincire hızlıca bir şekilde eklenebilir. Yaygın olarak kullanılan yöntemde, başlığın özet değerinin bir hedef değere eşit veya daha az olması şeklindedir. Yayıncı düğüm, blok başlığında (nonce değeriyle oynayarak) küçük değişiklikler yaparak çözümü elde etmeye çalışır. Bu işlem yüksek kaynak gereksinimi duyar. Bu sayede ağın ve zincirin güvenliği arttırılır. Çünkü kötü niyetli bir düğüm ağa geçersiz bir blok eklemek isterse, bu blok ve bundan sonraki tüm bloklar için bulmacayı yeniden çözmesi gerekmektedir [33].

Örnek olarak, SHA-256 güvenli özetleme algoritması kullanılarak aşağıdaki şartları sağlanması gereksin:

SHA256(“blockchain” + Nonce) = Özet değer “000000” ile başlamalıdır.

Bu örnekte “blockchain” değerine numerik nonce değeri eklenerek özet değeri hesaplanmaktadır. Hesaplanan özet değer “000000” ile başlamak zorundadır. Bulmacayı çözmek için bu şartları sağlayacak nonce değerini bulmak gerekmektedir.

SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
(çözüm değil)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10
(çözüm değil)

…

SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587
(çözüm)

Bu örnekte çözümü bulmak için 10730895 deneme yapmak gerekmektedir. Bu da görece eski bir donanımla 54 saniye sürmektedir. Bulmacanın zorluğunu arttırmak için gereken sıfır sayıları bir arttırılabilir(“0000000”).

SHA256("blockchain934224174") =
0x0000000e2ae7e4240df80692b7e586ea7a977eacbd031819d0e603257edb3a81

Bu durumda ise 934224174 deneme gerekmektedir. Bu da benzer bir donanımla 1 saat, 18 dakika, 12 saniye sürmektedir.

Yüksek hesap gücü gerektiren bulmaca, bir saldırganın birçok düğüm oluşturarak ağa saldırmasına (Sybil Attack) engel teşkil etmektedir. İşin ispatı yöntemi bunu, ağa etkilemek için gereken gücün odağını hesaplama gücüne kaydırarak ve rastlantısal bir sistemle birleştirerek yapmaktadır [35].

3.2.2 Sahipliğin ispatı (proof of stake)

Sahipliğin ispatı, işin ispatı yöntemine göre enerji tasarrufu sağlayan bir alternatiftir. Bu yöntem, ağa daha fazla yatırım yapmış kullanıcının sistemin başarılı olmasını isteyeceği fikrine dayanmaktadır [33]. Sahiplik genel olarak, sistemde sahip olunan kripto para miktarıyla ölçülmektedir. Yeni blokların yayınlanmasında kimin seçileceğine, hangi kullanıcın daha fazla hisseye sahip olmasına göre karar verilir. Yani daha fazla kripto para sahibinin, bir sonraki blok için seçilmesi ihtimali artmaktadır.

Bu modelde, yüksek hesaplama gücü gerektirecek işlemler gerçekleştirmeye gerek yoktur. Bu yüzden daha az kaynak kullanılmakta ve bu yöntemi kullanan bazı blockchain ağları ödüllendirme sisteminden vazgeçmiştir. Bu ağlarda tüm kripto para önceden basılır ve yatırımcılar arasında dağıtılır. Blok yayınlanması için gereken ödül ise kullanıcılar tarafından ödenen işlem ücretleriyle sağlanır. Bu mutabakat sistemin kullanan ağlarda, zengin yani daha fazla değere sahip olan kullanıcıların daha da zenginleşmesi tehlikesi vardır [36].

3.2.3 Yetki verilmiş sahipliğin ispatı (delegated proof of stake)

PoS ve DPoS arasındaki en büyük fark, PoS doğrudan demokrasi örneğiyken DPoS temsili demokrasi örneğidir. Ağdaki paydaşlar, blok oluşturma ve doğrulama için temsilciler seçerler. Bloğu onaylamak için daha az düğüm gerektiğinden, blok daha hızlı bir şekilde onaylanabilir. Blok boyutu, blok aralıkları gibi ağ parametreleri temsilciler tarafından ayarlanır. Bu yöntemin en büyük sorunu, kötü niyetli temsilcilerin seçilme ihtimalidir [33].

3.2.4 Practical byzantine fault tolerance – PBFT

Bu yapı adını Bizans İmparatorluğunda kullanılan bir yöntemden almaktadır. Bizans İmparatorluğunda, generaller gelen emirlerin gerçekten imparatora ait olup olmadığını anlamak için gelen emirleri yakındaki diğer generallere gönderir ve kendilerine ulaşan emirlere bakarmış. Şayet ellerindeki emirlerin çoğunluğu ile kendilerine ulaşan emir aynı ise emir doğru kabul edilmekteymiş.

Bu yapı blockchain ağlarında ise şu şekilde kullanılmaktadır: Ağdaki doğrulayıcı rolüne sahip her düğümde özel/açık anahtar ikilisi bulunmakta ve diğer düğümlerin açık anahtarlarını saklamaktadır. Her makine kendisine ulaşan işlemi kontrol eder ve onaylarsa imzalayarak ağ ile paylaşır. Şayet ağdaki diğer makineler de önceden anlaşılan oranda işlemlerin doğruluğunu onaylarsa mutabakat sağlanmış olur. Bu yöntemde; doğrulama sistemi sahiplik, hesaplama gücü gibi kavramlardan ayrılmaktadır ve sisteme dâhil her kullanıcının yeni blokların belirlenmesinde söz sahibi vardır. Bu da ağdaki her düğümün birbirinden haberdar olmasına ve yeni katılacak düğümlerin merkezi bir yapı tarafından onaylanmasına sebep olmaktadır. Bu yüzden bu mutabakat yöntemi, açık ağlardan ziyade özel ağlarda kullanılmaktadır. Hyperledger Fabric, bu mutabakat yöntemini kullanmaktadır. Çizelge 3.2'de uzlaşma yöntemlerinin karşılaştırılması gösterilmektedir [33].

Çizelge 3.2 : Uzlaşma yöntemlerinin karşılaştırılması.

Özellik	**PoW**	**PoS**	**PBFT**	**DPoS**
Düğüm Kimlik Yönetimi	Açık Ağ	Açık Ağ	İzin Gerektiren Ağ (Özel Ağ)	Açık Ağ
Enerji Tasarrufu	Yok	Kısmen	Var	Kısmen
Kötü Niyetli Düğümlere Karşı Direnç	Hesaplama Gücünün < 25%	Sahipliğin < 51%	Hatalı Kopyalar < 33.3%	Onaylayıcıların < 51%
Uygulama Örneği	Bitcoin	Peercoin	Hyperledger Fabic	Bitshares

3.3 Çakışma ve Çözüm Yöntemleri

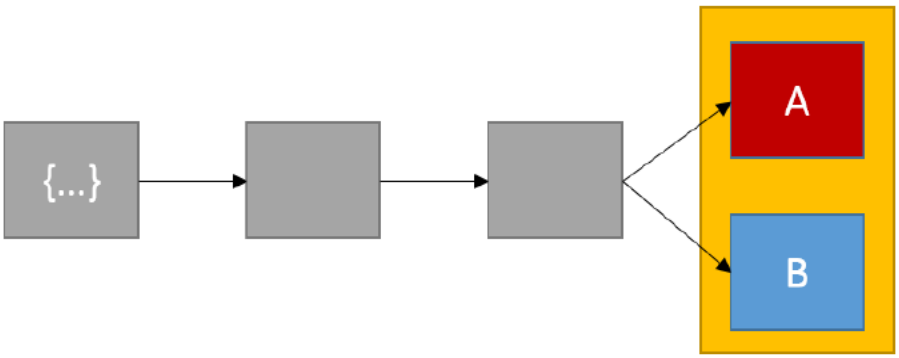
Özellikle açık blockchain ağlarındaki düğümler, yeni eklenecek blokları oluşturmak için birbiriyle yarışmaktadır. Bazı durumlarda, aynı anda iki farklı düğüm yeni bir blok üretimiyle karşımıza çıkabilir. Bu da herhangi bir anda iki farklı zincirin ortaya çıkmasına sebep olur. Zincirin tutarlılığa sahip olması için bu tür çakışmaların hızlıca çözülmesi gerekmektedir.

Daha önce tartışıldığı gibi, bazı blok zincir ağları için, yaklaşık olarak aynı anda birden fazla bloğun yayınlanması mümkündür. Bu, herhangi bir anda bir blockchain'in farklı sürümlerinin var olmasına neden olabilir. Bunlar, blockchain ağında tutarlılığa sahip olmak için çabucak çözülmelidir. Bu bölümde, bu durumların genellikle nasıl ele alınacağını tartışacağız.

Örneğin:

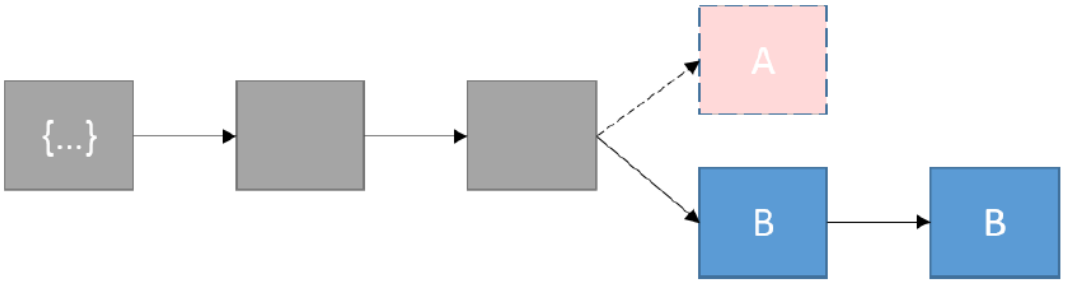
- Düğüm_ A 1, 2, 3 numaralı işlemlerle blokA'yı oluştursun ve ağdaki bazı düğümlere yayın yapsın.
- Aynı şekilde Düğüm_B 1, 2, 4 numaralı işlemlerle blokB'yi oluştursun ve bazı düğümlere yayın yapsın.

Böyle bir durumda çakışma oluşmaktadır. blok_A'da 3 numaralı işlem bulunurken 4 numaralı işlem bulunmamaktadır. Benzer şekilde blok_B'de 4 numaralı işlem bulunurken 3 numaralı işlem bulunmamaktadır. Çakışma yaşanan bir zincir örneği Şekil 3.1'de görülebilir.



Şekil 3.1 : Çakışma yaşanan bir zincir.

Bu durum geçici olarak ağda iki farklı zincir oluşmasına sebep olmaktadır. Bu iki zincir de geçerli ve doğrudur ancak zincirin bütünlüğü açısından ikisinin birden devam etmesi söz konusu olamaz. Böyle bir durumda ağ bir sonraki blok üretimini bekler. Bir sonraki blok hangi zincirde yayınlanırsa o zincir resmi zincir olarak seçilir. Yani en uzun zincir, doğru zincir olarak seçilmektedir. Reddedilen zincirdeki bloklar yetim kalırlar ve bu bloklardaki işlemler yeniden doğrulanarak zincire eklenmek için kuyruğa alınır. Merkezi bir yapı bulunmadığından dolayı, her bir işlem düğüm yerelinde saklanır. Şekil 3.2'de en uzun zincirin, asıl zincir olarak kabul edilmesi görülmektedir.



Şekil 3.2 : En uzun zincirin kabul edilmesi.

3.4 Çatallaşma

Her yazılım projesinde olduğu gibi blockchain ağlarında da yeni geliştirmelere, güncellemeler ve güvenlik yamalarına ihtiyaç vardır. Ancak blockchain ağının dağıtık mimarisinden dolayı güncelleme yapmak oldukça zorlaşabilir. Özellikle açık ağlarda güncellemeleri reddeden kullanıcılar olabilir. İzin gerektiren kapalı ağlarda böyle bir durumla karşılaşmak pek mümkün olmaz, çünkü düğümler güncelleştirmeyi almaya zorlanabilir.

Bir blockchain ağının protokolünde veya veri yapılarında yapılan değişikliklere çatallaşma (fork) adı verilir. Bunları geçici (soft) ve mecburi (hard) çatallaşma olarak ikiye ayırabiliriz. Geçici çatallaşmada, yapılan güncellemeler geçmişe doğru uyumlu olurken mecburi çatallaşmada böyle bir durum söz konusu değildir. Bu durumda zincirin birden çok sürümü oluşabilir.

3.4.1 Geçici çatallaşma

Bu tür bir çatallaşmada, güncellenmeyen düğümler güncellenmiş düğümlerle işlem yapmaya devam edebilir. Güncellenen düğümler zincire yeni blok ekleyebilirken, güncellenmeyenler yeni blok ekleyemezler ancak mutabakat süreçlerine dâhil olabilirler. Yani yeni eklenen blokları doğrulayabilirler.

3.4.2 Mecburi çatallaşma

Bu tür çatallaşmada, belirli bir blok numarasında tüm düğümlerin yeni güncellemeyi alması gerekmektedir. Güncellenmeyen düğümler zinciri okuyamayacak, yeni blok ekleyemeyecek veya onaylayamayacaktır. Güncellemeyi reddeden düğümler eski yazılım ve zincirle yollarına devam edebilirler ve bu durumda iki farklı zincir oluşmuş olur.

3.5 Akıllı Sözleşmeler

Akıllı sözleşme, belirlenen sözleşmenin şartlarını yerine getiren bilgisayar tabanlı bir işlem protokolüdür. Blockchain'de akıllı sözleşme, yayıncı düğümler tarafından otomatik olarak yürütülebilen bir kod parçasıdır [33].

Akıllı sözleşme terimi, Nick Szabo tarafından 1994 yılında “sözleşmenin şartlarını yerine getiren bilgisayar tabanlı bir işlem protokolü” olarak tanımlanmıştır. Akıllı

sözleşme tasarımının temel hedefleri, ortak sözleşme koşullarını (ödeme koşulları, borçlar, gizlilik) karşılamak, kötü niyetli durumları ve güvenilen aracılara olan ihtiyacı en aza indirmektir [37].

Akıllı sözleşmeyi yürüten tüm düğümler, aynı girdi parametreleriyle yürütmeden aynı sonuçları elde etmelidir. Elde edilen sonuçlar blok zincirine kaydedilir. Ek olarak, akıllı sözleşmeyi yürüten tüm düğümler, yürütme sonrasında elde edilen yeni durum hakkında hemfikir olmalıdır. Bunu başarmak için, akıllı sözleşmeler doğrudan kendisine aktarılanların dışındaki veriler üzerinde çalışmazlar [38].

Akıllı sözleşmelerin şu anda kullanımda olan geleneksel sözleşme yapılarına karşı çeşitli avantajlar bulunmaktadır:

- Akıllı sözleşmeler, genel olarak elle yürütülen süreçlere göre daha hızlıdır.
- Akıllı sözleşmeler, insan kaynaklı hatalara karşı daha dayanıklıdır.
- Akıllı sözleşmelerin dağıtık ağ yapısı üzerinde uygulanması, kötü niyetli yönlendirmelere karşı daha dirençli olmalarını sağlamaktadır.
- Akıllı sözleşmeler, güven için gerekli olan aracı kurumlara ihtiyacı azaltmaktadır.
- Akıllı sözleşmeler, daha düşük maliyetlidir.

Bunların dışında çeşitli dezavantajları da bulunmaktadır:

- İşlem Süresi: Günümüzdeki blockchain yapılarında işlemlerin doğrulanıp bloklara eklenmesi klasik veri tabanı teknolojilerine göre çok daha yavaş kalmaktadır.
- Geliştirme Zorluğu: Henüz yeni gelişen bir teknoloji olduğundan tasarlama, geliştirme, yükleme ve test etme aşamalarını daha verimli hale getirecek araç sıkıntısı bulunmaktadır.
- Dış Bilgiye Erişim: Akıllı sözleşmelerin sadece blockchain ağı üzerindeki bilgilere erişimi bulunmaktadır. Bu yüzden dış kaynaklardan bilgiyi getirecek güvenilir veri kaynaklarına ihtiyaç duyarlar. Bu tarz servislere Oracle (Kâhin) adı verilmektedir.
- Güvenlik: Her ne kadar blockchain ağları kriptografik olarak güvenli olsa da geliştirme aşamasında insan kaynaklı hatalara açıktır.

- Esneklik: Blockchain tabanlı akıllı sözleşmeler değiştirilemez yapısından dolayı, sözleşmeler geliştirilirken tüm olası senaryolar düşünülmelidir.

3.6 Blokchain Uygulama Alanları

Bitcoin'in elde ettiği başarıdan sonra blockchain teknolojisi üzerindeki genel algı, finans uygulamaları için uygun olduğu yönündedir. Ancak bu teknoloji diğer birçok alan için de uygulanabilir.

Çizelge 3.3'te gösterilen SWOT analizi ile blockchain teknolojisinin ne tür alanlarda kullanılabileceğine dair daha iyi fikir yürütülebilir [39].

Çizelge 3.3 : Blockchain SWOT analizi [39].

Güçlü Yönler	**Zayıf Yönler**
• Dağıtık esneklik ve kontrol • Merkezi olmayan ağ • Açık kaynak • Güvenlik ve kriptografi • Varlık ispatı • Yerel varlık yaratma • Dinamik ve akıcı değiş tokuş	• Kayıt defteri birlikte çalışabilirliğindeki eksiklikler • Zayıf kullanıcı deneyimi • Test edilmiş teknoloji eksikliği • Geliştirici araçlarındaki eksiklikler • Cüzdan ve anahtar yönetimi • Yetenek azlığı ve maliyetleri • Yeni teknoloji sağlayıcılarına olan güven eksikliği
Fırsatlar	**Tehditler**
• Düşük işlem maliyetleri • İş süreçlerinde hızlanma ve efektiflik • Dolandırıcılık işlemlerinde azalma • Sistemsel risklerde azalma • Parasal demokratikleşme • Yeni iş modelleri • Uygulamaların rasyonelleştirilmesi	• Yasal sınırlamalar • Siyasi aktörler • Teknoloji hataları • Kurumsal entegrasyon sınırları • Farklı blockchain sistemleri • Kayıt defteri çakışmaları • Yönetim eksikliği

Blokchain teknolojisinin çözüm aranacak bir sorun için uygun olup olmadığı, Amerika Birleşik Devletleri İç Güvenlik Departmanı Bilim ve Teknoloji Müdürlüğünce (DHS) oluşturulmuş, şekil 3.3'te görülen akış şemasıyla karar verilebilir [40].

Şekil 3.3 : Blockchain kullanmaya karar verme akış diyagramı.

Çeşitli endüstriler için olası blockchain kullanım senaryoları aşağıdaki gibidir [23]:

Finansal Hizmetler

- Uluslararası ödemelerde, karşı tarafın hükümlerini yerine getirememe riskini azaltarak daha hızlı, ucuz ve güvenli olabilir.
- Şartlara daha uygun ve daha iyi Müşteri Tanıma Sistemleri
- Uluslararası ticareti geliştirmek ve hızlandırmak için ticaret finansı blok zinciri.

Sağlık Hizmetleri

- Hastaları daha iyi eşleştirmek ve çift kayıtları önlemek için klinik kayıtların gerçek zamanlı olarak paylaşılması.
- Otomatik işlemler ve sigortacılar, denetçiler gibi çeşitli taraflar arasında bağlantı kurmak için akıllı sözleşmeler.

Kamu Hizmetleri

- Verimliliği arttırmak ve sahtekârlığı azaltmak için insanların kimliğinin, mülk ve araç gibi varlıkları üzerindeki mülkiyet ve işlem bilgilerinin tutulduğu dijital kayıt defterleri.
- Seçimlerde arttırılmış güvenlik ve şeffaflık.

Enerji ve Tabii Kaynaklar

- Akıllı sözleşmeler ile enerji ticareti ödemelerinin daha hızlı ve verimli yapılması.
- Tedarik zinciri süreçlerini iyileştirmek için petrol ve gaz işlemlerini yönetmek ve kayıt altına almak, tedarikçileri, nakliyatçıları, yüklenicileri ve yetkilileri blok zincirle bağlamak.

Teknoloji, Medya ve Telekom

- Müziğin güvenli özetinin saklanması, sahiplerin dijital kimliklerine bağlanması ve akıllı sözleşmeler yolu ile telif ödemelerinin kolaylaştırılması.
- Güvenlik sorunlarının azaltılmasına yardımcı olmak için, kriptografik biçimde çok sayıda loT aygıtı arasında veri depolama ve etkileşimi destekleme.

Tüketici ve Endüstriyel Ürünler

- Perakende satış, seyahat ve konaklamadaki sadakat puan programlarının daha iyi yönetimi.
- Daha az dokümantasyon ve otomatik ödeme ile araç satın alma ve kiralama sürecini kolaylaştırmak.
- Gelişmiş tedarik zinciri yönetimi, üretim başlangıcından son müşterinin kullanımına kadar ürünler arasında izlenebilirlik.

4. MEVCUT SEÇİM TEKNOLOJİLERİ VE SORUNLARI

Giriş bölümünde bahsettiğimiz mevcut seçim teknolojilerinin, seçim gereksinimleri bakımından çeşitli sorunları bulunmaktadır. Bu bölümde elle sayılan kâğıt oy pusulaları, kollu oy makinaları, delikli kart pusulaları, optik oy pusulaları, doğrudan kayıt eden elektronik oy makinaları ve internet üzerinden oylama tekniklerini daha ayrıntılı bir şekilde inceleyerek, seçim gereksinimleri ve diğer yönlerden sorunlarını ele alacağız.

4.1 Elle Sayılan Kâğıt Oy Pusulaları

Günümüzde de halen kullanılmakta olan kâğıt oy pusulaları, resmi makamlarca kontrol edilmekte ve belirlenen standartlara göre basılmaktadır. Aynı ebatlarda olan, standart şekilde basılan oy pusulalarının sayımı oldukça hızlı bir şekilde yapılabilmektedir. Ancak sayım aşamasında oldukça fazla insan gücüne ihtiyaç duyulmaktadır. Bu sistemde seçmen, oyunu kâğıt bir oy pusulasında genellikle bir mühür aracılığı ile belirterek kullanır. Sandıkta en azından kayıtlı seçmen sayısı kadar oy pusulası bulunmalıdır [41].

Oy verme işleminden, sayıma kadar insanlarca yapılmasından dolayı bu sistem insan hatalarına oldukça açıktır. Oy verme işlemi sırasında, yetersiz kalan talimatlar veya oy pusulasının kötü tasarımından dolayı seçmenin yanlış oy kullanması olasıdır [42]. Her ne kadar oy sayımı yasalarca belirlenen kurallara göre yapılıyor olsa da bazı durumlar için oy sayımı sübjektif bir şekilde yapılabilir. Ayrıca oyların sayımı, tutanaklara geçirilmesi ve transferi sırasında hileli işlemler uygulanabilir. Örneğin, oy sayımı esnasında seçimde yarışan her aday veya parti için sandıklarda en az bir kişinin bulunması gerekir. Bir parti veya aday herhangi bir sandıkta kontrolü ele geçirirse sayımı kendi lehlerine göre yapabilir. Buna ek olarak, kullanılmamış oy pusulalarını kendi lehlerine göre manipüle edebilir. Bu sistemdeki en büyük sorun insan faktöründen kaynaklanabilecek hatalar ve seçimleri yürüten organlara güven zorunluluğudur.

4.2 Kollu Oy Makinaları

Kollu oy makinalarında seçmen, bir makinanın karşısında adaylar arasından seçimini yaparak, ilgili kolu çeker ve oyunu verir. Bunun sonucunda, makinada ilgili adayla bağlantılı tekerlek hareket ederek, adayın oyunu bir attırır. Oy verme işlemi bitip sandıklar kapandıktan sonra, makine açılarak hangi adayın kaç oy aldığı tutanaklara geçirilir.

Bu makinaların kâğıt oy pusulalarına karşı birkaç avantajı bulunmaktadır. İlk olarak oy sayma işlemi birkaç saatten birkaç dakikaya inmektedir. Aynı zamanda kâğıt oy pusulalarında ortaya çıkan seçim hilelerinin önüne geçebilmektedir [43].

Kollu oy makinalarının sağladığı faydaların yanında dezavantajları da bulunmaktadır. En büyük dezavantajı oyların yedeğinin olmamasıdır. Herhangi bir şekilde yeniden sayım mümkün değildir. Makinada oluşabilecek bir arızada oylar yeniden sayılamaz. Buna ek olarak bazen kolların kasıtlı veya sehven yanlış etiketlendiği de görülmüştür. Ayrıca bu makinalar oldukça büyük, hantal ve karmaştır. Büyüklük ve hantallık makinaların taşınmasını oldukça zorlaştırmakta ve maliyetleri arttırmaktadır. Aynı zamanda makinaların üretimi ve bakım maliyetleri de bu sebeplerden yükselmektedir. Bunlara ek olarak makinaların karmaşıklığı test edilmelerini zorlaştırmaktadır [44].

4.3 Delikli Kart Pusulaları

Delikli kart pusulalarında adayların isimleri kartların üzerinde değildir. Kartlar üzerinde numaralar bulunur ve her bir numara bir aday ile ilişkilendirilmiştir. Genellikle, adayların isimleri ve isimlerinin yanında yuvarlak bir boşluk bulunan kitap benzeri rehber kartlar bulunur. Oy pusulası bu kitap benzeri rehberin sırtına yerleştirilir. Ardından seçmen oy vermek istediği adayın karşındaki deliğe bir iğne veya benzeri bir cisimle bastırarak altındaki oy pusulasını deler. Ardından oy pusulasını sandığa atarak oyunu kullanmış olur. Genellikle rehberin sağ tarafında aday isimleri bulunurken, sol tarafında delikler bulunur. Ancak “kelebek (butterfly)” oy pusulalarında rehberin sağ ve sol tarafında aday isimleri yer alırken, ortasında delikler bulunur. Bu durum kafa karıştırıcı olabilmektedir. Şekil 4.1’de delikli kart pusulası görülebilir.

Şekil 4.1 : Delikli kart pusulası.

Delikli kart pusulalarının iki önemli sorunu bulunmaktadır. Birincisi, kartların delinmesi sırasında ortaya çıkmaktadır. Öyle ki, oy pusulalarının temiz, anlaşılır ve doğru konumda delinmesinin bir garantisi bulunmamaktadır. Tam olarak delinmeden çukur oluşmuş, kartın bir parçasının sarktığı delikler görmek mümkündür. Amerika 200 genel seçimlerinde, Florida eyaleti Palm Beach ilçesinde bu sorunla karşılaşılmıştır. Verilen 433.043 oyun 6.358 geçersiz sayılmıştır [44]. İkinci sorun olarak, geçerli oyun belirlenmesinde sübjektif bir yorumlaya açık olmasıdır. Kartın tam olarak delinemediği ancak bir parçasının karta bağlı kaldığı durumlarda hangi oyların geçerli olacağı bir sorundur.

4.4 Optik Oy Pusulaları

Optik oy pusulaları, delikli oy pusulalarına bir alternatif olarak düşünülebilir. Bu sistem, üniversite giriş sınavlarındaki ve buna benzer testlerdeki sisteme benzemektedir. Seçmenler oy pusulasında, adayın karşılığına denk gelen boşluğu kurşun kalemle doldurarak oyunu kullanır. Bir makinada bu oyları saymak için pusulaları tarar. Sayma işlemi otomatik olarak yapıldığından oldukça hızlıdır.

Optik oy pusulaları da kâğıt oy pusulaları gibi oy verildikten sonra hileli bir şekilde değiştirilebilir. Bunun yanında, seçmenlerin makine üreticisinin belirttiği standartlar dışında oy kullanmasından dolayı, oylar geçersiz olabilir veya yanlış sayılabilir. Bunu önlemek için seçmenler oylarını verdikten sonra kontrol etmeleri amacıyla oy kabinlerine okuma cihazları konmaktadır. Seçmen oy verdikten sonra pusulayı bu cihaza okutur ve doğruluğunu kontrol eder. Ancak bu cihazları her seçim konumuna koymak maliyetlidir ve her zaman mümkün olmamaktadır. Bu cihazların olmadığı

yerlerde, optik ve delikli oy pusulalarında geçersiz oy oranları benzer çıkmaktadır [45].

4.5 Doğrudan Kayıt Eden Elektronik Oy Makinaları

Tipik bir Doğrudan Kayıt Eden Elektronik Oy Makinası, dokunmatik bir ekrandan oluşan bir bilgisayardır. Kesintisiz bir güç kaynağına bağlı olan bu bilgisayar, özel bir ağa bağlıdır. Oyun gizliliğini korumak için bir kabinde bulunur. Aslında bakılırsa bilgisayarlı bir kollu oy makinası olarak düşünülebilir. Oylar sisteme kaydedilir ve sonrasında özel ağ ile seçim yönetim sistemine yüklenir. Kollu oy makinasına benzerliğinden dolayı, benzer sorunlar bu makinalarda da yaşanmaktadır [46].

Bu makinalarda, kollu oy makinalarına benzer bir şekilde oyların yedeği tutulmaz. Bundan dolayı yeniden sayım mümkün değildir. Makinada meydana gelebilecek bir arıza durumunda, bu donanım veya yazılım kaynaklı olabilir, verilen oyların doğruluğu konusunda şüphe ortaya çıkar. Ayrıca bilgisayar tabanlı sistemler olduğundan, dışarıdan izinsiz bir müdahale gerçekleşebilir. Böyle bir durumda, müdahalenin fark edilerek oyların geçersiz sayılması en iyi senaryo olacaktır. Şayet müdahale fark edilmezse kâğıt, delikli kart ve optik oy pusulalarında olduğu gibi seçim hilesi yapmak mümkün olacaktır. Ayrıca bu makinalar için geliştirilen yazılımın güvenilir kurumlar tarafından denetlenmesi gerekmektedir.

4.6 İnternet Üzerinden Oylama

İnternet üzerinden oylamanın, bir diğer adıyla i-oylama, olağan akışında seçmenler internete bağlı herhangi bir bilgisayardan oy kullanabilirler. Bu teknoloji, doğrudan olmayan elektronik oylama olarak düşünülebilir. Bu yüzden doğrudan elektronik oylamanın sahip olduğu tüm sorunlar bu seçim teknolojisinde de görülmektedir. Bunun yanı sıra, doğrudan kontrol edilebilen bir makine üzerinden oy verme işlemi yapılmadığı için bu durumun ortaya çıkardığı sorunlar da beraberinde gelmektedir [47].

İnternet üzerinde oylama, seçmen katılımını artırabilen ve daha az maliyetlerle yapılabilen bir oylamadır. Aynı zamanda, oyların sayımı ve geçerliliğine karar verilmesi süreçlerinde, insan hatasına yer vermez ve daha hızlı oy sayımı yapılabilmektedir. Bununla birlikte, oy verme sürecinin şeffaflığı konusunda ciddi

kaygılar doğurabilir. Avrupa İyi Kod Uygulamaları (Code of Good Practice) ve Bakanlar Tavsiye Komitesi'ne (Committee of Minister's Recommendation) göre, devlet makamları, elektronik oy teknolojilerinin doğru, güvenli ve güvenilir bir şekilde işlev görmesini sağlamalıdır. Özellikle, sistemin düzgün çalıştığını kontrol etmek oylama sırasında mümkün olmalıdır. Arızalara ve kötü niyetli saldırılara karşı güvenilir olmalıdır [48].

İnternet üzerinden oylamanın en başarılı uygulaması tartışmasız Estonya'dır. 2015 yılındaki parlamento seçimlerinde oyların yaklaşık %30,5'i internet üzerinden kullanılmıştır. Sistemin ilk kez kullanıldığı 2007 yılı genel seçimlerinde kullanım oranı yaklaşık olarak %5 olmuştur. Aradaki 8 yıllık zamandaki artış oranı dikkate alındığında sistemin başarısı göz önüne serilmektedir [49].

5. BLOCKCHAİN AĞI ÜZERİNDE ELEKTRONİK OYLAMA

Blockchain teknolojisi ile oylama sistemi geliştirilirken, mevcut seçim sistemlerinin eksiklikleri giderilmeli ve seçim sisteminin gereksinimleri sağlanmalıdır. Bununla beraber oluşabilecek sorunlar en aza indirilmelidir. Model önerisinde bulunmadan önce seçim sistemi gereksinimlerini hatırlamakta fayda var:

- Tüm seçmenlerin eşit ve bir oy hakkının garanti altına alınması.
- Vekâleten veya başka bir seçmenin yerine oy kullanılamaması.
- Gizli ve meçhul oy kullanılması.
- Oy verme işlemine erişilebilirliğin tüm seçmenler için eşit olması.
- Oyların sayımı ve işlenmesinde açık ve şeffaf bir yöntemin izlenmesi.
- Seçim sonuçlarının, oy verme işlemi bitene kadar hiçbir şekilde takip edilememesi.
- Oyların yedeğinin bulunması ve yeniden sayımın mümkün olması.
- Oy pusulaları üzerinde herhangi bir değişim yapılamaması.
- Denetlenebilir ve güvenilir olması.

Yukarıda sayılan gereksinimlerin dışında, blockchain ağı üzerinde elektronik oylama modeli geliştirilirken bazı teknik detayların da göz önünde bulundurulması gerekmektedir. Bunlardan en önemlisi, blockchain ağının ağır yük altında yeterli performansı gösterebilmesidir. Performans metrikleri olarak bir işlemin onaylanma süresi ve saniyedeki işlem hacmi (TPS) düşünülebilir.

Model tasarımında bulunmadan önce, seçim sistemindeki aktörler ve kullanılacak teknolojinin iyice irdelenmesi gerekmektedir. Daha önceki bölümlerde, seçim sistemi için gerekli olan temel gereksinimler, blockchain teknolojisinin nasıl çalıştığı ve neler yapabileceği anlatıldı. Bu bölümde ilk olarak seçim sistemindeki aktörler ve bu aktörlerin görev, sorumluluk, yetki düzeyleri incelenecek. Ardından gereksinimler ve

aktörlerin rollerine göre nasıl bir blockchain teknolojisinin kullanılması gerektiği incelenecek. Son olarak ise blockchain tabanlı e-seçim model önerisinde bulunulacak.

5.1 Analiz

Genel olarak seçimlerde karşımıza 4 ana aktör çıkmaktadır. Bunlar düzenleyici kurum, siyasi partiler, seçmenler ve gözlemci kuruluşlardır. Düzenleyici kuruluş yasalarla belirlenmiş seçim sürecinin düzenlemekle ve yürütmekle sorumludur. Oy verme, oy sayımı ve oyların işlenmesi süreçlerinin yasalara uygun, adil ve şeffaf bir şekilde yapılmasından sorumludur. Siyasi partiler, gösterdikleri adaylar ile seçim yarışına katılırlar. Ayrıca parti mensubu üyeler aracılığıyla, oyların sayımı ve işlenmesi sürecine katılırlar. Politik ve siyasi güç elde etmek amacıyla seçimlerde hile yapabilir ve adil olmayacak eylemlerde bulunabilirler. Bu istenmeyen durumların engellenmesi gerekmektedir. Seçmenler oy verme işlemini mevcut seçenekler arasından veya bir tercih olarak geçersiz yapabilirler. Seçmenin oyu, kesinlikle seçmenle bağlantılı olmamalıdır. Yani hangi seçmenin, ne oy verdiği hiçbir şekilde takip edilememelidir. Aynı zamanda seçmen oy sayımı ve işlenmesi süreçlerine gözlemci olarak katılabilir. Gözlemci kuruluşlar seçim süreçlerinin yasalara uygun, adil, şeffaf ve hilesiz bir şekilde yürütüldüğüne emin olmak için bu süreçleri inceleyebilirler. Bunlar uluslararası kuruluşlar olacağı gibi sivil toplum kuruluşları da olabilir.

Blockchain ağlarında performansı etkileyen en önemli faktör uzlaşma yöntemidir. Uzlaşma yönteminde kullanılan algoritma, işlemin ne kadar sürede zincire kaydedileceğini, aynı anda kaç işlem üzerinde çalışılabileceğini ve işlemin onaylanması için ne kadar kaynak gerekeceğini belirler. Açık ve izin gerektirmeyen blockchain ağlarında, katılımcılar birbirlerine güvenmezler. Böyle bir ortamda, katılımcılar arasındaki güveni tesis etmek uzlaşma yönteminin güvenilirliğine bağlıdır. Bu tür ağlarda, uzlaşma yöntemi olarak yüksek işlem gücü gerektiren algoritmalar seçilir. Bu sayede kötü niyetli bir katılımcının zinciri istediği gibi değiştirmesi için gereken bilgisayar gücü pratikte hiç bir zaman sağlanamaz. Bu durum güven ortamını tesis ederken, performans bakımından bazı fedakârlıklara sebep olmaktadır. Özel ve izin gerektiren ağlarda ise düğümler ağa bir izin sonucunda katıldığından dolayı, öncesinde kendi aralarında belirli bir güveni tesis etmiş olurlar. Ayrıca seçim süreçlerinin sınırları, yasalar ve kurallar ile çizildiğinden isteyen herkesin blockchain ağına katılması düşünülemez. İzin gerektiren ağlarda belirli bir güven önceden

sağlandığından, uzlaşma algoritmaları yüksek işlem gücü gerektirmezler. Bu sayede, ağın performansı daha yüksek olabilmektedir. Ancak bu tür ağların bir dezavantajı bulunmaktadır. Ölçeklenebilirlik bakımından açık ve izin gerektirmeyen ağlara göre daha kötü bir performans sergilerler. Neyse ki, bu durum blockchain seçim ağı düşünüldüğünde bir problem teşkil etmemektedir. Böyle bir ağı gerçeklemek için yüzlerce düğüme ihtiyaç yoktur. Aktörlerin görev ve sorumluluklarını yerine getirecek kadar düğümün ağda olması yetmektedir. İzinsiz ağların birçoğunda İşin İspatı (Proof of Work - PoW) ailesinden uzlaşma yöntemleri kullanılırken, izin gerektiren ağlarda Bizans Hata Dayanıklılığı (Byzantine Fault Tolerance - BFT) ailesinden uzlaşma yöntemleri kullanılmaktadır. Marko Vukolic tarafından, 2016 yılında yapılan PoW ve BFT yöntemlerinin karşılaştırılması Çizelge 5.1'deki gibidir [50].

Çizelge 5.1 : PoW ve BFT uzlaşma yöntemleri karşılaştırması

	PoW Uzlaşma Yöntemleri	**BFT Uzlaşma Yöntemleri**
Düğüm Kimlik Yönetimi	Açık, tamamen dağıtık	İzin gerektiren, düğümler diğer tüm düğümlerin kimliklerini bilmeli
Uzlaşma Kesinliği[1]	Yok	Var
Ölçeklenebilirlik (Düğüm sayısı bakımından)	Yüksek (Binlerce düğüm)	Sınırlı (20'ye kadar düğüm ile test edildi)
Ölçeklenebilirlik (İstemci sayısı bakımından)	Yüksek (Binlerce istemci)	Yüksek (Binlerce istemci)
Performans (İşlem hacmi)	Sınırlı (Zincir çatallaşmalarından dolayı)	Yüksek (Saniyede on binlerce işlem)
Performans (Gecikme)	Yüksek (Çoklu blok onayından dolayı)	Yüksek (İletişim ağı gecikmesiyle sınırlı)
Güç Tüketimi Verimliliği	Çok kötü	İyi
Kötü Niyetli Düğümlere Karşı Direnç	<= %25 hesaplama gücü	<= %33 oylama gücü
Ağ Eşzamanlılık Varsayımları	Fiziksel saat zaman damgaları	Uzlaşma güvenliği için gerekmiyor
Doğruluk Kanıtı	Yok	Var

Yapılan analize göre gereksinimleri karşılayacak blockchain teknolojisi, aktörlerin görev ve sorumluklarına göre okuma/yazma işlemlerinin yetkilendirilmesini

[1] **Uzlaşma Kesinliği:** Blok zincirinde çakışma sonucu çatallaşma meydana gelebilir ve kısa olan zincir reddedilir. Bu durumda uzlaşma kesinliği var denemez.

yapabilecek yetenekte olmalıdır. Ayrıca özel ve izin gerektiren bir ağ olmalıdır. Performans gereksinimlerinden dolayı, kullanılacak uzlaşma yöntemi yüksek hesaplama gücü gerektirmeyecek bir yöntem olmalıdır. Neyse ki, özel ve izin gerektiren bir ağda, düğümler izinle ağa katıldığından öncesinde bir güven tesis edilmiş olmakta ve yüksek hesaplama gücü gerektiren bir uzlaşma yöntemine ihtiyaç duyulmamaktadır. Blockchain ağının doğası gereği, ağa eklenen her işlemde, işlemin kim tarafından gönderildiği ve işlem içeriği görüntülenebilmektedir. Okuma işlemi sadece belirli yetkiye sahip düğümlere veya rollere verilse bile, bu yetki kötüye kullanılarak seçmenin tercihi takip edilebilir. Gizli oy esasını sağlayabilmek için, blockchain teknolojisinin dışında, bilinmezliği sağlayabilecek bir yöntem kullanılmalıdır. David Chaum tarafından, 1983 yılında, izlenemez ödemeler için ortaya atılan "Blind Signatures" şifreleme yöntemi bunu sağlayabilir [51].

5.2 Blind Signatures

Bu şifreleme yöntemini anlamak için uzaktan mektupla oy kullanma örneği kullanılabilir. Örneğin, uzaktan, mektupla oy verme işlemi gerçekleştirilmek zorunda olunan bir seçim olsun. Her bir seçmen oylarının gizliliği konusunda emin olmak isterken, aynı zamanda oylarının sayıldığından da emin olmak istesin. Buna çözüm olarak astarında karbon kopya kâğıdı bulunan zarflar düşünülebilir. Her bir seçmen oyunu bu zarfların içine yerleştirir. Ardından bu zarfı, üzerinde kendi iade adresi bulunan ikinci bir zarfın içine yerleştirir ve düzenleyici kuruma postalar. Düzenleyici kurum içerdeki zarfı çıkarır ve imzalar. Düzenleyici kurum her bir zarfı aynı imza ile imzalamalıdır. Ardından geri göndereceği adresi kontrol eder ve bu adresin geçerli bir seçmen olduğuna emin olur. İmzaladığı karbon astarlı zarfı, yeni bir zarfa koyarak seçmene geri postalar. Seçmen zarfı açar ve içindeki karbon astarlı zarfı çıkarır. Karbon astarlı zarfın imzalandığından emin olur ve içindeki oy pusulasını çıkarır. Seçim günü, oy pusulasını geri dönüş adresi olmayacak şekilde yeni bir zarfa koyarak meçhul bir şekilde postalar. Yeni zarfları alan düzenleyici kurum oy pusulalarının kendi tarafından imzalandığını kontrol eder. Ardından sayım işlemini açık bir şekilde yapar. Şayet seçmen, kâğıdın dokusu gibi kendi oy pusulasını tanıyacak küçük bir ayrıntı hatırlarsa kendi oyunu teyit edebilir. Düzenleyici kurum hiçbir zaman oy pusulasını görmediğinden hangi pusulanın kime ait olduğunu bilemeyecektir. Bu noktada düzenleyici kurumun, kendisine gelen her zarf için aynı imzayı kullanması

gerekmektedir. Çünkü her zarf için farklı bir imza kullanırsa, oyların sayımı sırasında hangi pusulanın hangi seçmene ait olduğuna dair bir bağlantı kurulabilir [51].

5.2.1 Blind RSA signatures

Blind signature şemalarından uygulaması en kolay olanı RSA imzalamaya dayanmaktadır. Bu şemaya göre akış 5 adımdan oluşur. Bunlar RSA anahtarlarının yaratılması, karıştırma, imzalama, çözme ve doğrulamadır.

RSA Anahtarlarının Yaratılması [52]

1. İmzacı p ve q olmak üzere rasgele iki büyük asal sayı seçer.
2. Ardından $n = pq$ ve $\lambda(n) = lcm(\lambda(p), \lambda(q)) = lcm(p - 1, q - 1)$ değerlerini hesaplar.
3. $1 < e < \lambda(n)$ ve $gcd(e, \lambda(n)) = 1$ olacak şekilde bir e tamsayısı seçer. Yani e ve $\lambda(n)$ aralarında asaldır.
4. $d \equiv e\text{^}(-1) \pmod{\lambda(n)}$ eşitliği için d değerini bulur.
5. e açık anahtar katsayısı olarak yayınlanır.
6. d özel anahtar katsayısı olarak saklanır.

Karıştırma (Blinding)

1. Kullanıcı m mesajı seçer.
2. n den küçük ve aralarında asal olacak $\mathbb{Z}_n^*$ kümesinden bir τ pozitif tam sayısı seçer.
3. $\alpha = (r^e \cdot H(m) \cdot mod(n))$ değerini hesaplar ve imzacıya gönderir. $H(x)$ SHA-256 gibi tek yönlü, güvenli bir özet fonksiyonudur.

İmzalama (Signing)

1. α değerini alan imzacı, $t = (\alpha^d \cdot mod(n))$ değerini hesaplar ve kullanıcıya gönderir.

Çözme (Unblinding)

1. t değerini alan kullanıcı, $s = (r^{-1} \cdot t \cdot mod(n))$ değerinin hesaplar. s değeri imzacının imzasıdır.

Doğrulama (Verifying)

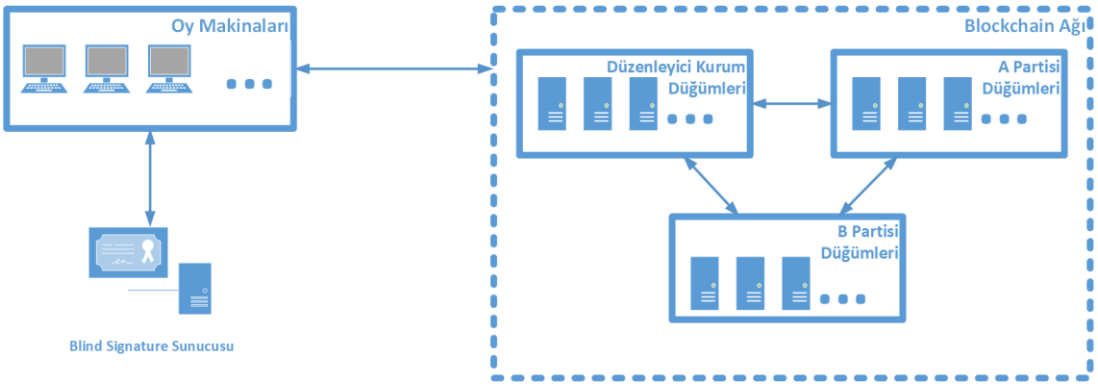
1. (s, m) imza, mesaj çifti $s^e \equiv H(m) \cdot mod(n)$ denkleminin doğruluğuna bakılarak kontrol edilebilir.

5.3 Blockchain Tabanlı E-Seçim Modeli

Blockchain tabanlı e-seçim modeli geliştirilirken, seçim gereksinimleri, seçim sürecindeki aktörler, aktörlerin görev ve sorumlulukları ile blockchain teknolojisinin sağlaması gereken performans kıstasları dikkate alınmıştır. Model üç aşamadan oluşmaktadır: Kurulum, Oy Verme, Oyların Sayımı ve Sonuçların İlanı. Kurulum aşamasında düzenleyici kurum blockchain ağının ve gerekli olacak diğer sistemlerin kurulumunu yapar. Blockchain ağına seçmen, parti ve aday, şifreleme anahtarları gibi varlıkları kaydeder. Oy verme işleminde, seçmenler istemci uygulamalar aracılığı oy seçiminde bulunurlar. Bu adımda blind signature yöntemiyle oylar meçhul ve güvenli bir şekilde imzalanır. Oylar, denetleyici kurum ve siyasi partilerin ağdaki düğümleri aracılığı ile onaylanarak şifrelenmiş şekilde zincire kaydedilir. Oyların sayımı ve sonuçları ilanı aşamasında, zincirdeki şifrelenmiş oylar şeffaf bir şekilde çözülerek sayılır. Bu aşamada seçmenler oylarının sayılıp sayılmadığını kontrol edebilir. Sayma işlemi bittikten sonra sonuçlar ilan edilir.

5.3.1 Kurulum

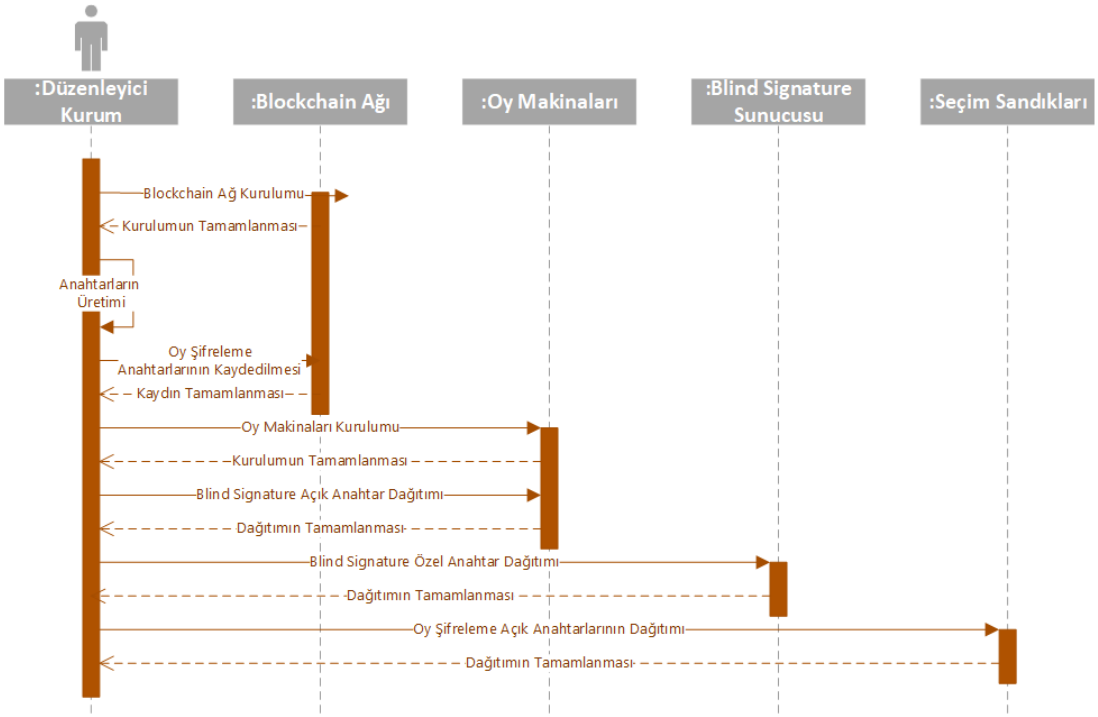
Bu aşamada düzenleyici kurum blockchain ağının kurulumunu yapar. Blockchain ağında bulunacak düğümlerin bir kısmı düzenleyici kurumun sahipliğinde olacakken, bir kısmı da siyasi partilerin sahipliğinde olacaktır. Bu sayede seçime giren her siyasi parti, düzenleyici kuruluş ile beraber oyların onaylanmasında söz sahibi olacaktır. Bu noktada herhangi bir aktörün, ağın bütünlüğünü tehlikeye atacak düğüm sayısına erişmemesine dikkat edilmelidir. Örneğin, uzlaşma yöntemi olarak BFT seçilirse, herhangi bir aktörün düğüm sahiplik oranının hiçbir zaman %33'ü geçmediğine emin olmak gerekir [53]. Bu orandan daha fazla düğüme sahip bir siyasi parti, siyasi hırs veya şantaj için düğümlerini kapatarak ağın bütünlüğünü tehlikeye atabilir. Şekil 5.1'de Oy Makinları, Blockchain Ağı ve Blind Signature Sunucu arasındaki etkileşim görülebilir.



Şekil 5.1 : Model bileşenleri arasındaki etkileşim.

Ağın kurulumu tamamlandıktan sonra, ağa gerekli varlıkların yüklemesi yapılır. Bunlar; seçim bölgeleri, sandıklar, adaylar, kayıtlı seçmen bilgileri gibi seçimle alakalı varlıklardır. Bu aşamada, düzenleyici kuruluş oyların gizliliğini sağlamak için blind signature yönteminde kullanılacak açık ve özel anahtar çiftini de üretir. Buna ek olarak seçmen sayısı kadar açık ve özel anahtar çifti de üretilmelidir. Bu anahtarlar, oylar blokchain ağına yazılırken şifrelemek için kullanılır.

Oyların şifrelenmesinde kullanılacak açık anahtarların, seçim öncesinde her sandığa dağıtılması gerekmektedir. Sandıklardaki açık anahtarlar, seçmenlere oy verme işlemi öncesinde rasgele bir şekilde verilir ve seçmen bu anahtarı oyunu şifrelemek için kullanır. Bu noktada açık anahtarların seçmenlerle bağlantı kurulamayacak şekilde dağıtılması gerekmektedir. Seçmen kendisine verilmiş olan saçık anahtarı oy verme işlemi bitene kadar saklayarak, oyunun sayılıp sayılmadığını kontrol edebilir. Oy verme işlemi bittiğinde, her bir açık anahtarın özel anahtarı açıklanır ve bu özel anahtarlar kullanılarak çözme işlemi yapılır. Bu sayede oy verme işlemi bitene kadar seçim sonuçlarını gözlemlemek mümkün olmamaktadır. Oyların şifrelenmesinde kullanılan anahtarlar zincire yazılarak, akıllı sözleşmeye eklenecek bir kuralla, oy verme işlemi bitene kadar okunamaması sağlanır. Şekil 5.2'de kurulum aşaması UML Sekans diyagramı görülebilir.



Şekil 5.2 : Kurulum aşaması UML Sekans diyagramı.

5.3.2 Oy verme

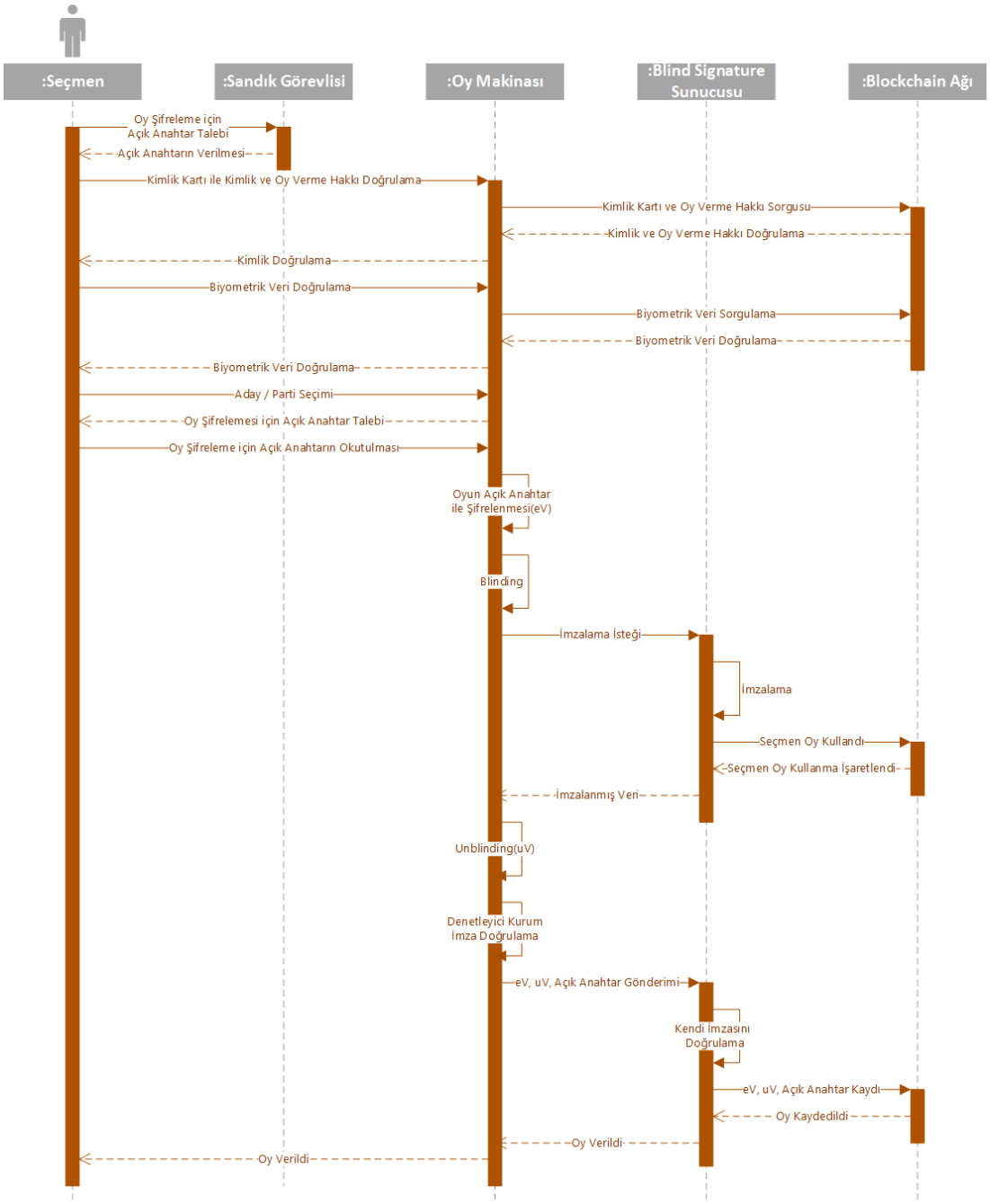
Bu aşamada seçmen oy verme işleminde bulunur. İlk olarak seçmen seçim sandığına gider ve görevli memur kendisine kapalı bir zarf içinde, oyunu şifrelemek için kullanacağı açık anahtarı verir. Bu anahtar, kare kod şeklinde bir kâğıda bastırılabilir. Ardından oy verme makinasının başına geçer. İlk olarak kimlik kartını okutur ve seçmenin oy verme hakkına sahip olup olmadığı belirlenir. Oy verme hakkı belirlenirken daha öncesinde oy verip vermediğine de zincir üzerinden bakılır. Ardından biyometrik bir veriyle kendisini yeniden doğrulatır. Örneğin bu veri parmak izi olabilir. Biyometrik veri ile iki aşamalı doğrulama yapılarak, vekâleten oy kullanmanın önüne geçilir. Ardından seçimini yapar ve kendisine verilmiş olan açık anahtarı okutur. Bu noktada, oyu bu açık anahtarla şifrelenir. Seçmen aynı açık anahtar ile oy verme işlemi tamamlandıktan sonra oyunun sayılıp sayılmadığını kontrol edebilir. Sonraki adım olarak blind signature ile doğrulama gelmektedir.

Blind signature için kullanılacak olan özel ve açık anahtar çifti daha önceden üretilmiştir ve açık anahtar her makinaya önceden yüklenmiştir. İstemci oy makinasında, açık anahtar ile karıştırma (blinding) işlemi yapılır. Karıştırılan mesaj imzalanmak üzere düzenleyici kurumun sunucularına gönderilir. Bu esnada, işlemi yapan seçmen bilgisi de gönderilir. Oy tercihi şifrelenmiş ve karıştırılmış olduğu için

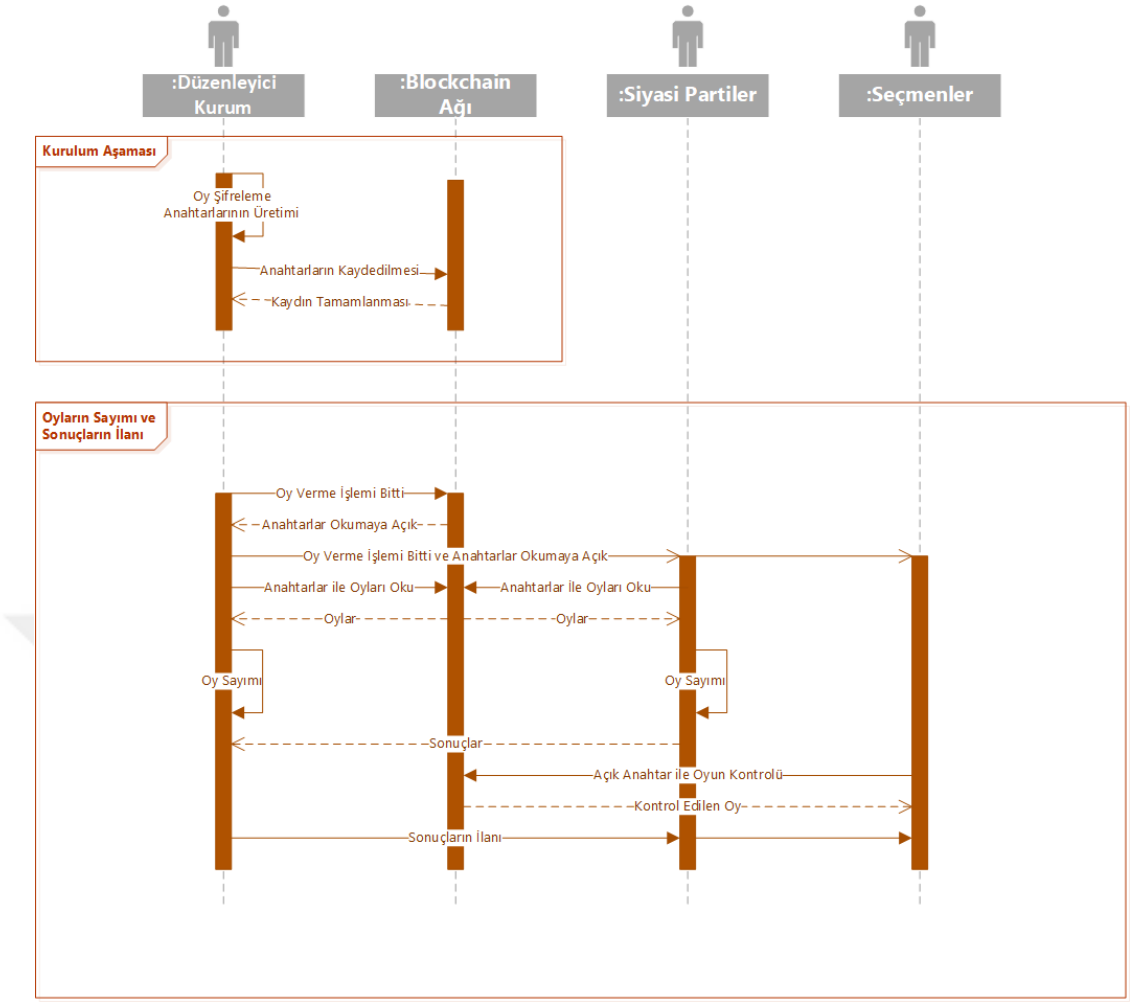
seçmenin tercihi tahmin edilemez. Düzenleyici kurum, ilk olarak ilgili seçmenin imzalama isteğinde bulunduğu bilgisini zincire kaydeder. Bu sayede her seçmenin sadece bir kez oy kullandığı garanti altına alınır. Ardından özel anahtarı ile karıştırılmış mesajı imzalar ve istemci oy makinasına geri gönderir. Oy makinası imzalanmış mesajı çözer (unblinding) ve düzenleyici kurum tarafından imzalanıp imzalanmadığını kontrol eder. Ardından makine çözülmüş mesajı, asıl mesajı ve şifreleme de kullanılan açık anahtarı düzenleyici kurumun sunucusuna gönderir. Asıl mesaj, her seçmene verilmiş olan açık anahtar ile şifrelenmiş olan oy tercihidir. Düzenleyici kurum, asıl mesaj ve çözülmüş mesajı karşılaştırarak kendisi tarafından imzalandığını onaylar. Ardından asıl mesajı ve açık anahtarı zincire ekler. Açık anahtar bilgisi, şifre çözme işlemi yapılırken ilgili özel anahtarı bulmak için kullanılır. Oy verme aşaması Şekil 5.3'de gösterilmektedir.

5.3.3 Oyların sayımı ve sonuçların ilanı

Son aşama oyların sayımı ve sonuçların ilanıdır. Bu aşama oy verme işlemi bittikten sonra başlar. İlk olarak, seçmenlerin oy verirken oylarını şifrelemek için kullanmış olduğu anahtarların ilgili özel anahtar çiftlerinin açığa çıkarılmasıyla başlar. Bu anahtar çiftleri blok zincirde tutulmaktadır. Bu anahtarların güvenliğini sağlamak için akıllı sözleşmeye bir kural eklenir. Bu kurala göre oy verme işlemi bittikten sonra ilgili anahtarlar okunabilir. Şifrelenerek kaydedilmiş olan oylar, şifrelemede kullanılan açık anahtarın ilgili özel anahtarıyla çözülür ve gerçek değerleri okunur. Bu aşamada seçmenler, düzenleyici kurum tarafından sağlanacak bir istemci uygulama ile oylarının sayılıp sayılmadığını kontrol edebilir. Bunun için ellerindeki açık anahtarın ilgili özel anahtarını bularak, oylarının gerçek değerlerine ulaşırlar ve kontrol ederler. Oyların gerçek değerleri çözüldükten sonra oy sayımı başlar. Oy sayımı işlemi bittikten sonra yasalarla belirtilen kurallara göre seçimi kazanan adaylar/siyasi partiler belirlenir ve ilan edilir. Kuralların akıllı sözleşmeler aracılığı ile yürütülmesine gerek yoktur. Oyların değerlerine göre düzenleyici kurum tarafından yürütülebilir. Oyların değerleri blockchain ağında tüm katılımcılara açık bir şekilde olduğundan sağlaması yapılabilir. Oyların sayımı ve sonuçların ilanı aşaması UML Sekans diyagramı Şekil 5.4'te gösterilmektedir.



Şekil 5.3 : Oy verme aşaması UML Sekans diyagramı.



Şekil 5.4 : Oyların sayımı ve sonuçların ilanı aşaması UML Sekans diyagramı.

6. SONUÇ VE ÖNERİLER

Bu çalışma kapsamında, blockchain tabanlı elektronik seçim sistemi geliştirilmiştir. Blockchain teknolojisinin özelliklerinden yararlanılarak seçim gereksinimlerini sağlayacak model ortaya çıkarılmıştır. Blockchain teknolojisinin yetersiz kaldığı alanlarda, blind signature gibi şifreleme yöntemleri kullanılmıştır. Bu sayede seçim gereksinimlerini sağlayan güvenilir ve şeffaf bir model ortaya konmuştur.

6.1 Kullanılan Yöntemler

Çalışmanın başında ilk olarak, seçim sistemi teknolojilerinin gereksinimleri incelenmiştir. Çeşitli ulusal ve uluslararası raporlar ve çalışmalar incelenerek, bir seçim sisteminde olması gereken azami gereksinimler ortaya çıkarılmıştır. Ardından blockchain teknolojisi ayrıntılı bir şekilde incelenmiştir. Bu teknolojinin nasıl çalıştığı irdelenmiş ve hangi alanlarda ne gibi faydalar sağladığı saptanmıştır. Blockchain teknolojisinin, hangi kıstaslar altında ne gibi değişiklikler yapılarak kullanılması gerektiği ortaya konulmuştur. Bunun ardından, dünya üzerinde yaygın olarak kullanılan seçim sistemi teknolojileri incelenmiştir. Bu teknolojilerin, seçim sistemi gereksinimleri bakımından analizi yapılmış, güçlü ve zayıf yanları ortaya konmuştur.

Analizi yapılan seçim gereksinimlerine göre blockchain tabanlı elektronik seçim modeli oluşturulmuştur. Model oluşturulurken, gereksinimlere göre nasıl bir blockchian teknolojisi kullanılacağı belirtilmiştir. Blockchain teknolojisinin yetersiz kaldığı alanlarda, çeşitli şifreleme yöntemlerinden faydalanılmış ve gereksinimleri karşılayacak bir model tasarlanmıştır.

6.2 Elde Edilen Sonuçlar

Geliştirilen model ile bu çalışmanın başında belirtilen seçim gereksinimleri sağlanmıştır.

Tüm seçmenlerin eşit ve bir oy hakkının garanti altına alınması: Oy kullanmaya uygun seçmenler ve oy kullanmış olan seçmenlerin bilgisi blockchain ağına kaydedilmiştir. Blockchain ağında zincire kaydedilen işlemlerin değiştirilmesi veya silinmesi mümkün olmadığından dolayı, oy kullanma hakkına sahip seçmenlerin hakları garanti altına alınmış ve birden fazla oy kullanmalarının önüne geçilmiştir.

Vekâleten veya başka bir seçmenin yerine oy kullanılamaması: Seçmenler oy kullanmadan önce iki aşamalı kimlik doğrulaması yapması gerekmektedir. Bu aşamalardan birinde biyometrik veri kullanılarak, başka bir seçmenin yerine oy kullanmanın önüne geçilmiştir.

Gizli ve meçhul oy kullanılması: Blockchain ağı doğası gereği, ağa erişimi olan herkes tarafından okunabilmektedir. Bu yüzden oyların gizliliği, sadece blockchain teknolojisini kullanarak kesin bir şekilde sağlanamaz. Bu noktada blind signatures yöntemi kullanılarak oyların gizliliği sağlanmıştır.

Oy verme işlemine erişilebilirliğin tüm seçmenler için eşit olması: Bedensel engellerinden dolayı bazı seçmenlerin seçim günü sandığa erişimleri imkânsız veya oldukça zor olmaktadır. Elektronik bir seçim sistemi tasarlandığından dolayı dijital cihazlarla gezici seçim sandıkları oluşturulabilir ve bu sandıklar, sandıklara erişim sorunu yaşayan seçmenlere ulaştırılabilir.

Oyların sayımı ve işlenmesinde açık ve şeffaf bir yöntemin izlenmesi: Blockchain ağının doğası gereği, ağa erişimi olan herkes ağdaki veriyi okuyabilmektedir. Bunun sayesinde, ağa erişimi sağlanan denetleyici kuruluş, siyasi partiler ve gözlemci kuruluşlar oylara şeffaf bir şekilde erişebilmektedir. Ayrıca, ağdaki onaylayıcı düğümler denetleyici kuruluş ve siyasi partiler arasında dağıtılmıştır. Böylece oyların kaydedilmesi sırasında tüm paydaşların sürece katılması sağlanmıştır.

Seçim sonuçlarının, oy verme işlemi bitene kadar hiçbir şekilde takip edilememesi: Blockchain ağına erişimi olan herkes zincirdeki veriyi okuyabilmektedir. Bu durum, seçim sonuçlanmadan önce zincirdeki oyların okunarak, seçmenlerin yanlış yönlendirilmesine sebep olabilir. Bunun önüne geçmek için her seçmenin oyu rasgele dağıtılan özel/açık anahtar çiftiyle şifrelenmiştir. Şifrelenmiş oyları çözecek özel anahtarlar ise seçim sonuçlanınca açıklanacağından, oy verme işlemi sırasında sonuçları tahmin etmenin önüne geçilmiştir.

Oyların yedeğinin bulunması ve yeniden sayımın mümkün olması: Zincirin bir kopyası ağdaki tüm düğümlerde bulunmaktadır. Böylece ağa dâhil olan tüm paydaşlarda her bir oyun yedeği bulunmaktadır. Ancak oyların dijital olarak kopyasının bulunması bazı paydaşlar ve halk tarafından yeterli bulunmayabilir. Bu durumda önerilen model genişletilerek oy makinaları tarafından dijital olarak imzalanmış, kâğıt oy pusulaları da kullanılabilir.

Oy pusulaları üzerinde herhangi bir değişim yapılamaması: Blockchain ağında zincire kaydedilen bir veri değiştirilemez veya silinemez. Bundan dolayı verilmiş olan oyların üzerinde bir değişiklik yapmak mümkün değildir.

Denetlenebilir ve güvenilir olması: Ağa erişimi olan herkes zinciri okuyabilir. Bu sayede tüm süreç denetlenebilir ve güvenilir olmaktadır.

6.3 Öneriler

Sunulan model blockchain teknolojisin getirmiş olduğu avantajlardan dolayı oldukça güvenlidir. Ancak bu durum oyların zincire yazılmasından sonraki süreçleri kapsamaktadır. Modelde yer alan istemci makinaların güvenliği, en büyük sorunu oluşturmaktadır. İleriki çalışmalarda bu makinaların güvenilir olmasını sağlayacak standartlar belirlenebilir.

Oyların yedeği ağa katılmış olan tüm düğümlerde bulunmaktadır. Bu yüzden teknik olarak başka bir yedeğe ihtiyaç duyulmamaktadır ancak halkın ve paydaşların blockchain teknolojisini tam olarak kavraması ve anlaması beklenemez. Bu durumda, önerilen modele karşı duyulan güven azalabilir. Bunun önüne geçmek için oy makinaları tarafından dijital olarak imzalanmış kâğıt oy pusulaları da seçim sürecine dâhil edilebilir.

Genel seçimlerde on milyonlarca seçmen oy kullanmaktadır. Bu sayı, bazı ülkeler için yüz milyonlara da çıkabilmektedir. Blockchain teknolojisinin bu ağır işlem hacmi yükünü kaldırabileceğinden emin olmak gerekir. Bundan sonraki çalışmalarda performans kıstasları belirlenerek, blockchain teknolojisinin bu kıstasları sağlayıp sağlayamadığı araştırılabilir.

KAYNAKLAR

[1] **Eulau, H., Gibbins, R., & Webb, P. D.** (22 Ocak 2015). Election. Alındığı tarih: 08 Kasım 2018, Adres: https://www.britannica.com/topic/election-political-science

[2] **Election.** (07 Kasım 2018). Alındığı tarih: 08 Kasım 2018, Adres: https://en.wikipedia.org/w/index.php?title=Election&oldid=867704365

[3] **Jones, D. W.** (2003). The evaluation of voting technology. *Secure electronic voting* (ss. 3-16). Springer, Boston, MA.

[4] **Nakamoto, S.** (2008). Bitcoin: A peer-to-peer electronic cash system.

[5] **Ayed, A. B.** (2017). A conceptual secure Blockchain-based electronic voting system. *International Journal of Network Security & Its Applications, 93*.

[6] **Brent, P.** (2006). The Australian ballot: Not the secret ballot. Australian Journal of Political Science, 41(1), 39-50.

[7] **Haber7.** (t.y.). 27 yıl sonra en kısa oy pusulası! Alındığı tarih: 08 Kasım 2018, Adres: http://www.haber7.com/guncel/haber/2636308-27-yil-sonra-en-kisa-oy-pusulasi

[8] **Smith, E.** (21 Mayıs 2012). It's Put Up or Shut Up Time as Filing Week Begins. Alındığı tarih: 08 Kasım 2018, Adres: https://washingtonstatewire.com/its-put-up-or-shut-up-time-as-filing-week-begins

[9] **Wikimedia Commons.** (t.y.). File:Votomatic 2000 Palm Beach County 011.JPG Alındığı tarih: 08 Kasım 2018, Adres: https://commons.wikimedia.org/wiki/File:Votomatic_2000_Palm_Beach_County_011.JPG

[10] **Benadida.** (08 Kasım 2006). My Day as an Election Warden in Boston. Alındığı Tarih: 08 Kasım 2018, Adres: https://benlog.com/2006/11/08/my-day-as-an-election-warden-in-boston

[11] **Krimmer, R.** (2012). The evolution of e-voting: why voting technology is used and how it affects democracy. *Tallinn University of Technology Doctoral Theses Series I: Social Sciences, 19.*

[12] **Waddell, K.** (01 Eylül 2016). How Electronic Voting Could Undermine the Election. Alındığı Tarih: 08 Kasım 2018, Adres: https://www.theatlantic.com/technology/archive/2016/08/how-electronic-voting-could-undermine-the-election/497885

[13] **Heiberg, S., & Willemson, J.** (Ekim 2014). Verifiable internet voting in Estonia. *Electronic Voting: Verifying the Vote (EVOTE), 2014 6th International Conference on* (ss. 1-8). IEEE.

[14] **Haber, S., & Stornetta, W. S.** (Ağustos 1990). How to time-stamp a digital document. *Conference on the Theory and Application of Cryptography* (ss. 437-455). Springer, Berlin, Heidelberg.

[15] **Anderson, R.** (Ekim 1996). The eternity service. *Proceedings of PRAGOCRYPT* (Say. 96, ss. 242-252).

[16] **Schneier, B., & Kelsey, J.** (Ocak 1998). Cryptographic Support for Secure Logs on Untrusted Machines. *USENIX Security Symposium* (Say. 98, ss. 53-62).

[17] **Buterin, V.** (202014). A next-generation smart contract and decentralized applicatiation platform. *white paper*.
[18] **Mevzuat** (t.y.) SeSeçimlerin Temel Hükümleri Ve Seçmen Kütükleri Hakkında Kanun**..** Alındığı tarih: 10 Kasım 2018, Adres: http://www.mevzuat.gov.tr/MevzuatMetin/1.4.298.pdf
[19] **Strasbourg,** (22 Ocak 2007) European Commission for Democracy Through Law (Venice Commission), *Opinion No. 399 / 2006*.
[20] **Gritzalis, D. A.** (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, 21(6), 539-556.
[21] **Council of Europe.** (2016). *Using international election standards : Council of Europe handbook for civil society organisations. Strasbourg:* Council of Europe Publishing. (s.82)
[22] **Grewal-Carr, V., & Marshall, S.** (2017). Blockchain: Enigma. Paradox. Opportunity (Deloitte).
[23] **DELOITTE** (2017). Blockchain - A Technical Primer. Deloitte Insights. Alındığı tarih: 14 Kasım 2018, Adres: https://www2.deloitte.com/content/dam/insights/us/articles/4436_Blockchain-primer/DI_Blockchain_Primer.pdf
[24] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (s. 7)
[25] **Election.** (11 Kasım 2018). Alındığı tarih: 14 Kasım 2018, Adres: https://en.wikipedia.org/w/index.php?title=Observable_universe&oldid=868358448
[26] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (s. 8)
[27] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 9-10)
[28] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (s. 11)
[29] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 12-13)
[30] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 14-15)
[31] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 15-17)
[32] **Szydlo, M.** (Mayıs 2004). Merkle tree traversal in log space and time. *International Conference on the Theory and Applications of Cryptographic Techniques* (ss. 541-554). Springer, Berlin, Heidelberg.
[33] **Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H.** (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on* (ss. 557-564). IEEE.
[34] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (s. 18)
[35] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 19-21)
[36] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 21-23)

[37] **Literature Review on Reaction Time,** Alındığı tarih: 15 Kasım 2018, Adres: www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[38] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (ss. 32-33)

[39] **Furlonger, D., & Valdes, R.** (2017). *Practical blockchain: a Gartner trend insight report.* Alındığı tarih: 14 Kasım 2018 Adres: https://haas.campusgroups.com/htc/get_file?eid=139611897577441f06512fc062b0a63e

[40] **Yaga, D., Mell, P., Roby, N., & Scarfone, K.** (2018). Blockchain technology overview. *NISTIR, 8202.* (s. 42)

[41] **Jones, D. W.** (2003). The evaluation of voting technology. *Secure electronic voting* (ss. 3-4). Springer, Boston, MA.

[42] **Cranor, L. F.** (2003). In search of the perfect voting technology: No easy answers. *Secure Electronic Voting* (ss. 25-26). Springer, Boston, MA.

[43] **Cranor, L. F.** (2003). In search of the perfect voting technology: No easy answers. *Secure Electronic Voting* (s. 20). Springer, Boston, MA.

[44] **Jones, D. W.** (2003). The evaluation of voting technology. *Secure electronic voting* (s. 6). Springer, Boston, MA.

[45] **Cranor, L. F.** (2003). In search of the perfect voting technology: No easy answers. *Secure Electronic Voting* (s. 23). Springer, Boston, MA.

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

[47] **Jones, D. W.** (2003). The evaluation of voting technology. *Secure electronic voting* (s. 14). Springer, Boston, MA.

[48] **Council of Europe.** (2016). *Using international election standards : Council of Europe handbook for civil society organisations. Strasbourg:* Council of Europe Publishing. (s.77)

[49] **Trechsel, A. H., Kucherenko, V. V., & Sılva, F.** (2016). *Potential and challenges of e-voting in the European Union.* (s. 27)

[50] **Vukolić, M.** (Ekim 2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *International Workshop on Open Problems in Network Security* (ss. 112-125). Springer, Cham.

[51] **Chaum, D.** (1983). Blind signatures for untraceable payments. *Advances in cryptology* (ss. 199-203). Springer, Boston, MA.

[52] **Rivest, R. L., Shamir, A., & Adleman, L.** (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 21(2), 120-126.

[53] **Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M. H.** (Eylül 2018). Platform-independent secure blockchain-based voting system. *International Conference on Information Security* (ss. 369-386). Springer, Cham.

ÖZGEÇMİŞ

Ad Soyad: Doğa Barış ÇAKMAK

Doğum Yeri ve Tarihi: Çorlu, 17.10.1991

E-Posta: cakmakdo@itu.edu.tr

Lisans: İTÜ Bilgisayar Mühendisliği

Yüksek Lisans: Bilişim Uygulamaları

Mesleki Deneyim ve Ödüller:

Tipster-Service-GmbH – Yazılım Mühendisi (Ocak 2019 – …)

SİM Yazılım ve Bilişim Hizmetleri – Yazılım Mühendisi (Mart 2018 – Ocak 2019)

İnnova Bilişim – Uygulama Geliştirme Uzmanı (Nisan 2016 – Mart 2018)

İTÜ BİDB – Yazılım Mühendisi (Mart 2014 – Nisan 2016)

Yayın ve Patent Listesi:

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR

▪ **Çakmak, D.B.,** Karaçuha, E., 2019: Blockchain Based E-Voting. *International Conference on Electrical Engineering and Computer Science*, Mayıs 1-4, 2019 Saraybosna, Bosna Hersek.