ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DOKTORA TEZİ

ELEKTRONİK OYLAMALAR İÇİN BLOK ZİNCİRİNE DAYALI GÜVENLİ BİR OYLAMA MODELİ

Ruhi TAŞ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2022

ÖZET

Doktora Tezi

ELEKTRONİK OYLAMALAR İÇİN BLOK ZİNCİRİNE DAYALI GÜVENLİ BİR OYLAMA MODELİ

Ruhi TAŞ

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Ömer Özgür TANRIÖVER

Elektronik oylama sistemlerinde güvenlik ve güven en önemli konulardır. Bu nedenle bu sistemlerde anonimlik, güvenlik, gizlilik ve güvenilirliği sağlamak için kriptografik prosedürlerin kullanılması gerekmektedir. Son yıllarda blok zinciri, merkezi olmayan uygulamalar aracılığıyla veri depolama ve iletimini güvence altına almak için en yaygın kullanılan yöntemlerden biri haline gelmiştir. E-oylama sistemlerinin blok zinciri ile entegrasyonu uygulama alanlarından biri olarak önerilmektedir. E-oylama sistemlerinde özellikle güvenlik ve veri manipülasyonu hala büyük bir sorun olarak görülmektedir. Bu modelde, yöneticilerin veya madencilerin blok zinciri yapısı nedeniyle normalde erişilebilen veriler olan seçim sonuçlarını ön izlemesi engellenmesi sağlanarak güvenli bir oylama modeli sunulmuştur. Seçim sonuçlarında meydana gelebilecek manipülasyonları önlemek için çift katmanlı bir şifreleme modeli de önerilmiştir. Bu sayede oylama sırasında olası manipülasyonların da önüne geçilebilmektedir. Oylama sonuçlarının güvenilirliği içinse tüm paydaşların katılımı ile seçim sonuçlarının doğrulanması sağlanmıştır. Önerilen model ile seçmenlerin mahremiyeti sağlanmakta, merkezi bir otoriteye ihtiyaç duyulmamakta ve kaydedilen oyların değiştirilmeden, dağıtık bir yapıda saklanmaları saklanarak güvenli bir oylama modeli oluşturulması önerilmiştir.

Ocak 2022, 107 sayfa

Anahtar Kelimeler: Blok Zinciri, Elektronik Oylama, Akıllı Sözleşmeler, Ethereum, Bitcoin

ABSTRACT

Ph.D. Thesis

A BLOCKCHAIN BASED SECURE E-VOTING SYSTEM

Ruhi TAŞ

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. Ömer Özgür TANRIÖVER

Security and trust are the most important issues in electronic voting systems. Therefore it is necessary to use cryptographic procedures to ensure anonymity, security, privacy and reliability in these systems. In recent years, blockchain has become one of the most commonly used methods for securing data storage and transmission through decentralized applications. E-voting is one of these application areas. However, data manipulation is still seen as a major problem in e-voting systems. In this model, administrators or miners are prevented from previewing election results which are normally accessible data due to the blockchain structure. A double-layer encryption model is proposed and tested to prevent manipulations that may occur with the election results. It is ensured that the election results can be counted after the participation of all stakeholders at the end. In this way, potential manipulations may be prevented during the election period. As a result of the model, the privacy of voters is ensured, no central authority is needed and the recorded votes are kept in a distributed structure.

January 2022, 107 pages

Keywords: Blockchain, Electronic Voting, Smart Contract, Ethereum, Bitcoin

ÖNSÖZ ve TEŞEKKÜR

Çalışmalarımı yönlendiren, araştırmalarımın her aşamasında bilgi, öneri ve yardımlarını esirgemeyerek engin fikirleriyle yetişme ve gelişmeme katkıda bulunan danışman hocam Sayın Dr. Öğr. Üyesi Ömer Özgür TANRIÖVER'e, çalışmalarım sırasında önemli katkılarda bulunan ve yönlendiren hocalarım Sayın Prof. Dr. İlhan KOŞALAY'a ve Dr. Öğr. Üyesi Bülent TUĞRUL'a, ayrıca tez süresince gösterdiği sabırla, destekle ve sürekli yanımda olan aileme, eşim Özlem Elif'e, yaşama sevinçlerim kızım Pelin'e ve oğlum Bartu'ya, ayrıca tez çalışmalarımda gerekli kolaylığı ve desteği sağlayan değerli iş arkadaşlarıma en derin duygularla teşekkür ederim.

Anneme,

Ruhi TAŞ

Ankara, Ocak 2022

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler

C_i	Seçmen
CL_i	Aday kimlik no
E_{id}	Seçim kimlik no
N	Düğüm sayısı
P	Rastgele asal sayı
V_i	Kayıtlı seçmen
λ	En küçük ortan bölen
S	Gizli veri

Kısaltmalar

ABI	Application Binary Interface
AES	Advanced Encryption Standard
AP	Access Point
API	Uygulama programlama ara yüzü (Application Programming Interface)
ARP	Address Resolution Protocol
B2B	Business to Business
BFT	Bizans hata toleransı (Byzantine Fault Tolerant)
DApp	Merkezi olmayan Uygulama (Decentralized Application)
DDBMS	Distributed Database Management System
DES	Data Encryption Standard
DLT	Dağıtılmış Defter Teknolojileri (Distributed Ledger Technologies)
DNS	Domain Name Server
DPoS	Delege edilen teminat kanıtı (Delegated Proof of Stake)
DRE	Direct-Recording Electronic

DSA	Digital Signing Algorithm
DVTYS	Dağıtılmış Veri tabanı Yönetim Sistemi
ECDSA	Elliptic Curve Digital Signature Algorithm
EIP	Ethereum Improvement Proposal
EVM	Ethereum Virtual Machine
FHE	Fully Homomorfic Encryption
HTTP	Üst Metin transfer protokolü (Hypertext Transfer Protocol)
HTTPS	Güvenli üst metin transfer protokolü (Hypertext Transfer Protocol Secure)
IoT	Nesnelerin interneti (Internet of Things)
IP	İnternet protokolü (Internet protokol)
LAN	Local Area Network
MAC	Media Access Control
MD	Message Digest
MIT	Massachusetts Institute of Technology
MITM	Man in the Middle Attack
NPM	Node Package Manager
P2P	Eşler arası (Peer to Peer)
PBFT	Practical Byzantine Fault Tolerant
PHE	Partially Homomorphic Encryption
PoS	Teminat kanıtı (Proof of State)
PoV	Proof of Vote
PoW	İş kanıtı (Proof of Work)
RC5	Rivest Cipher 5
REST	Representational State Transfer
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm

SHE	Somewhat Homomorphic Encryption
UML	Unified Modeling Language
VITA	Virginia Information Technologies Agency
VPN	Virtual Private Network

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

1.1 Elektronik Oylama

Adil ve tarafsız bir seçim herkesin arzu ettiği bir durumdur. Günümüzde hala oylama işlemleri sırasında, sayım işlemlerinde ve sonuçların açıklanmasında bazı şaibelerin yaşandığı tespit edilmektedir (Achieng ve Ruhode 2013, Bishop ve Hoeffler 2016, Water 2017, Shukla vd. 2018). İlk zamanlardan bugüne kadar seçim süreçlerinde, seçimin yapıldığı zamanın ihtiyaçlarına ve gelişmelere bağlı olarak bazı değişimler yaşandığı belirtilmektedir. Teknolojik gelişmelerin her alanda yenilikler sunduğu, oylama süreçlerine de katkı sağlayabileceği bir gerçektir. Teknolojik yeniliklerinin oylama sistemlerindeki insana bağlı hataları azaltabileceği, bazı kolaylıklar getireceği düşünülmektedir (Blanc 2007). Bu kapsamda seçim sistemlerine de bazı ek özellikler ve çözümler önerilmektedir. Ağ teknolojisinin gelişmesi sonucunda, kolay seçim organizasyonu, hızlılık ve düşük maliyet sağlayacağı düşünülerek elektronik cihazların farklı çeşitleri de uygulama alanında yer almaktadır. Biyometrik kimlik doğrulamadan (Gentles ve Sankaranarayanan 2012), uzaktan oylamaya (Volkamer ve McGaley 2007), kiosk sistemlerine (Gurubasavanna vd. 2019) kadar birçok teknolojik özellik oylama sistemlerine dâhil edilerek denenmiş ve geliştirilmeye de devam etmektedir. Ayrıca, elektronik oylama sistemlerinin uzaktan oylamaya da izin vererek katılımı kolaylaştırdığı belirtilmektedir. Seçimlere daha fazla katılımın sağlanması açısından da önemli olduğu vurgulanmaktadır. Bununla birlikte, e-oylama sistemlerinde de kendisine özgü bazı güvenlik ihlalleri yaşanabildiği belirtilmektedir. Yolsuzluk ve seçmen kimliğine bürünme, dolandırıcılık veya mükerrer oy kullanımı gibi farklı ihlallerin yaşandığı belirtilmiştir (Zheng Wei ve Wen 2018, Fan vd. 2021). Oyların saklanması esnasında kurcalanmaya açık olması ihtimalinin varlığı her zaman önemli bir problem olduğu belirtilmektedir (Blanc 2007).

Son yıllarda bazı gelişmiş demokrasilerde de seçimlere katılımın azaldığı görülmektedir. Avrupa'da 2014 yılı ortalama seçimlere katılım oranı % 42,5 seviyelerine kadar düştüğü görülmüştür. Elektronik oylama sistemlerinin katılım

oranını artırabileceği değerlendirdiğinden bu türü sistemlerin kullanımı ilgi görmektedir. Bu nedenle, elektronik sistemlerin entegre edildiği seçim süreçlerinin, sorunlara çözüm olabileceği değerlendirilmektedir (Trechsel vd. 2016). Estonya'da 2007 yılında gerçekleştirilen internet oylamasının geniş katılım sağlaması açısından başarılı bir uygulama örneği olarak gösterilmektedir. Elektronik seçim sırasında ilk kez elektronik kimlik kartı ile oy verenlerin sayısının %39'lara çıktığı görülmüştür (Clarke ve Martens 2016, Kitsing 2011), ayrıca Norveç, 2011 ile 2013 arasında denemeler yapmıştır, ancak güvenlik endişeleri nedeniyle 2014 yılında projeyi iptal etmiştir. Bu tür uygulamaların hayata geçirilmesi kararları söz konusu olduğunda, sistemin verileri güvence altına alma kabiliyetine ve potansiyel saldırılara karşı savunma yeteneğine her zaman şüpheyle yaklaşılmıştır (Bull vd. 2018). E-oylama sistemleri merkezi yönetilen veri tabanına sistemleri ile çalışmaktadır. Ayrıca şeffaf olmayan uygulamaların kullanılması, denetim eksikliği ve bütünlük korumasının olmaması gibi eksiklikler güven ortamını zedelemektedir (Fan vd. 2021).

Bu tez çalışmasında, son zamanların önemli gelişmelerinden biri olan blok zinciri altyapısıyla bütünleşmiş, güvenli elektronik oylama hizmeti modeli oluşturulması hedeflenmiştir. Blok zinciri teknolojisini seçim sistemiyle birleştirerek, merkezi olmayan, oylama sürecinde şeffaflık ve verilerin değiştirilmesine karşı dayanıklılık sağlayan özelliklere sahip, daha güvenilir bir çözüm sunmak hedeflenmiştir.

Tez mevcut oylama sistemlerinin kısa özetleri ile başlamaktadır. Daha sonra, blok zinciri teknolojisinin ne olduğu, nerelerde ve nasıl kullanıldığı hakkında teknik bilgiler verilmiştir. Ayrıca, mevcut oylama uygulamalarındaki potansiyel sorunların ve tehditlerin analizi yapılmıştır. Sonraki bölümde önerilen modelin tanımlaması yapılarak uygulanan şifreleme yöntemleri açıklanmıştır. Son olarak, önerilen blok zinciri modellemesin nasıl kullanılabileceği değerlendirilmiştir.

1.2 Tezin Amacı ve Önemi

Elektronik oylama sistemleri özellikle kullanılan oyların toplanması ve sayılmasında önemli kolaylıklar sağlamaktadır. Ayrıca işitsel ve görsel yardımlarla oylama

kolaylığını artırmaya yardımcı olması açısından da önemlidir. Ancak, elektronik sistemlerin kullanımıyla birlikte bazı riskleri de beraberinde getirdiği tespit edilmektedir (Bishop ve Wagner 2007). Siber saldırılar en ciddi problemlerin başında gelmektedir. Yetkisiz erişim ve hileli yönlendirme gibi durumlar yaşanabilmektedir. Bu sebeple çevrimiçi oylamada verilerin toplanmasının, saklanmasının ve güven ortamının oluşturmanın önemini ortaya çıkarmaktadır.

Bu tez çalışmasında geleneksel elektronik oylama sistemlerinden farklı olarak, sistematik bir şekilde blok zincirinin elektronik oylama sisteminde kullanılması süreçleri araştırılmıştır. Sonrasında, elektronik oy verme sistemlerine olan güvensizlik önyargısını azaltmayı amaçlayan, blok zinciri ile bütünleşik bir oylama sistemi önerilmiştir. Blok zinciri altyapısı kullanımıyla, diğer oylama sistemlere göre daha güvenli veri saklama imkânı sunan, manipülasyonlara dayanıklı ve denetlenebilirlilik özelliklerinin artırıldığı bir sistem hedeflenmiştir. Bu sistem, oyların daha güvenli saklanmasına ve oyların ifşa olmasını engellemeye yardımcı olmak amacıyla çift katmanlı şifreleme tekniği içermektedir. Önerilen sistemle, oy pusulalarını saymak ve oylama sonucunu yayınlamak için merkezi bir otorite olmadan sayımların yapılabilmesi mümkündür. Oy pusulalarının gizliliğini ve şifrelenmiş kayıtlar üzerinden sayma işleminin gerçekleştirilmesini sağlayan homomorfik şifreleme metodu kullanılmıştır. Sistemin evet/hayır gibi ikili oylama ve daha fazla seçenekli sistemlerle de uyumludur. E-oylamada seçim gizliliğini korumanın yanı sıra bağımsız birimlerce sonuçların alternatif olarak doğrulanabildiği bir seçim sistemi önerilmiştir.

1.3 Tezin Özgün Değeri

Bu çalışma kapsamında blok zinciri tabanlı elektronik oylama sistemleri makaleleri sistematik haritalama yöntemi ile incelenmiştir. Blok zinciri sistemlerindeki problemler ve fırsatlar hakkında incelemeler yapılmıştır. Bu yöntemle tespit edilip incelen makaleler; genel konular, mahremiyet, bütünlük, fikir birliği ve kripto paraya dayalı çalışmalar olarak kategorize edilmiştir (Taş ve Tanrıöver 2020). Bu

çalışmaların %40.63'ü nün genel özelliklerle birlikte protokol önerilerinde bulundukları tespit edilmiştir. Blok zinciri sistemlerinin mevcut seçim sistemlerinde hâkim olan bazı sorunlara çözüm sağlayabileceği belirlenerek sunulmuştur. Ayrıca, blok zinciri uygulamalarında en sık vurgulanan problemlerin gizliliğinin korunması, ölçeklenebilirlik ve işlem hızı olarak öne çıktığı belirlenmiştir. Blok zinciri çerçevelerinin oylama uygulamalarında kullanılabilmesi için hala iyileştirmelere ihtiyacı olduğu kanaati oluşmuştur. Bu çalışmada, elektronik oylama sistemlerinin yaygın olarak kullanılmasındaki güvensizliklerden biri olan oyların manipülasyonlara açık olmasını engellemek için blok zinciri altyapısını kullanan dağıtık veri yapılı seçim sistemi önerilmiştir. Blok zincirinin özelliklerini oylama sistemine entegre ederek değiştirilemez, izlenebilir, dağıtık yapıda veri senkronizasyonuna izin veren ve güvenlik işlemlerinin iyileştirmesi sağlanmıştır. Sistemin yönetim kolaylığı sağlaması, oy pusulalarında mükerrerliği önlemesi, doğru ve güvenilir bilgi sağlaması hedeflenmiştir.

Geliştirilen uygulama Ethereum blok zinciri teknolojisini kullanan (Dapp – Decentralized Application) bir oylama uygulaması olarak geliştirilmiştir. Uygulama bileşenlerinde klasik oylama özellikleri, elektronik sistemler, veri tabanı ve blok zinciri yapısını kullanan hibrid bir yapı önerilmiştir. Her bir sistemin kendi üst düzey özelliklerinin kullanılması önerilmiştir. Önerilen sistemde verilerin değiştirilememezliği ve anonimliği sağlanmıştır. Blok zinciri sisteminde açık olan verilerin ifşa olmasını engellemek için verilerin düğümlerde tek başına anlamsız hale getirilmesi sağlanmıştır. Saklanan verilerin anonimliği için öncelikle Pailler homomorfik (Paillier 1999) şifreleme yöntemi kullanılmıştır. Daha sonrasında da bu şifreli verilerin Shamir yöntemi (Shamir 1979) ile parçalanarak düğümlerde dağıtılması sağlanmıştır. Bu sayede veri yedekliliği ile birlikte kullanılan oyların sayımı sırasında bağımsız birimler tarafından da sürecin takip edilmesi sağlanmıştır. Ayrıca, sonuçların açıklaması sırasında belirli sayıda düğümün bir araya gelmesi zorunlu hale getirilerek çapraz kontrol mekanizması oluşturulmuştur. Tekil seçmen ve başkasının yerine oy kullanmayı engellemek için sistemde kullanılan altyapılarda

sistemlerden bağımsız olarak biyometrik kimliklerin dağıtılması, seçim kayıt ve oy verme sırasında bu sistemlerin elektronik okumalarının yapılması önerilmiştir.

Tasarlanan sistemin uygulama senaryosunda sistem gereksinimleri tanımlanmış ve performans değerlendirmesi yapılmıştır. Seçmenin biyometrik kontrollü kimlik kartı ile oy verme hakkının olup olmadığının kontrollü ile farklı kişilerin oy kullanmalarının engellenmesi önerilmiştir.

1.4 Tezin İçeriği

Tez şu şekilde düzenlenmiştir. Giriş bölümünün ardından oylama sistemlerine genel bakış, sonrasında blok zinciri teknolojisinin temel kavramlarının incelendiği bölüm yer almaktadır. Bu bölümün devamında mevcut elektronik oylama sistemlerinin araştırmaları yapılmıştır. Literatürdeki blok zinciri çalışmaları detaylı olarak ele alınmış, bu konudaki eğilimler tartışılmıştır. Beşinci bölümde ise elektronik oylamalardaki eksiklikler belirtilmiş, sonrasında da blok zinciri sisteminin olası katkıları incelenmiştir. Sonraki bölümde önerilen sistemin modellemesi ve çalışma prensibi detaylandırılarak incelenmiştir. Son bölümde tez araştırmasının sonuçları ve öneriler paylaşılmıştır.

2. OYLAMA SİSTEMLERİ ÖZELLİKLERİ

Oylama, bir grup insanın, listelenen yarışmacılar veya konular arasından belirli kurallara ve düzenlemelere göre tercih etmesini içeren bir sistemdir. Bu sebeple, oylama yöntemleri yaygın olarak iki süreçte kullanılmaktadır: biri seçim faaliyetleri, diğeri ise önemli konularda karar vermektir. Seçimde oy verme davranışı, genel olarak, seçmenlerin, seçim sürecinde, tercihlerini göstermek için seçilen kişiye oy verdikleri davranışı ifade etmektedir. Kısaca, seçim; birden fazla seçenek arasından birinin seçilmesi olarak tanımlanmaktadır (Türk 2006). Yıllardır seçim, yaşamın her aşamasında kullanılmaktadır. Özellikle günümüzde, modern dünyada seçimin vazgeçilmez bir unsur olduğu bilinmektedir. Birçok farklı amaç için kullanılmakla birlikte en önemli yönü demokratik yönetime temel katkı sağlamasıdır (Riemann ve Grumbach 2017, Zhang 2020). Seçimler neticesinde, seçmenlerin yönetimdeki sorumlu liderleri belirleyerek temsil edilmelerine yardımcı olmaktadır (Haydaroğlu ve Çevik 2016). Ülkemizde ilk genel seçim 1876 yılı sonunda başlayıp 1877 yılında tamamlanan uzun bir sürede gerçekleştirilmiştir (Alkan 2006). O günlerden günümüze kadar birçok kez yerel ve genel seçimler tekrarlanmıştır. Günümüze kadar geçen bu süreçte, seçim mevzuatında zamanın ihtiyaçlarına ve teknolojik gelişmelerine göre çeşitli kanuni düzenlemeler yapılmıştır (Anonim 2020). 26.4.1961 tarihli ve 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkındaki kanun Türkiye'de ki mevcut seçimleri organize eden kanundur. Sonraki yıllarda yapılan düzenlemelerle birlikte elektronik seçim sisteminin de kullanılabileceği belirtilmektedir (Anonim 2021). Tüm dünya genelinde de geleneksel oylama sisteminin geçmişi son derece eskidir. Kâğıt oy pusulalarından başlar, ardından E-oylama ve son olarak I-oylamaya kadar devam etmektedir.

2.1 Kâğıt Temelli Oylama

Dünyada uzun yıllardır kâğıt temelli oylama sistemi seçimlerde oy kullanma yöntemi olarak kullanılmaktadır. Güney Avustralya ve Victoria'da 1856'da uygulamaya konulan yöntem ilk oylama sistemini temsil etmektedir. Gizli oylama olarak ta bilinen

bu oylamalarda kâğıt oy pusulaları kullanılmıştır (Yi ve Das 2020). Kâğıt temelli oylama sistemleri, seçmenlerin oylarını denetlenen bir seçim istasyonundaki bir oylama kabininde işaretleyerek, kilitli bir oy sandığına atarak yapması olarak gerçekleştirilmektedir. Bu durum, oylamanın gizliliğini sağlamakta ayrıca hiçbir seçmenin harici bir etmenden etkilenmemesini garanti etmektedir. Dahası, kapalı sandıkların açılması ve sayılması, halkın ve resmi gözlemcilerin gözetimi altında yapılabilmektedir. Ancak, büyük bir seçmen kitlesine sahip ülkelerin genel seçimlerinde, kâğıt tabanlı oylama sistemi ile bir seçim yapmak bazı zorlukları barındırmaktadır. Özellikle nihai sonuçları açıklamak için günlere, hatta haftalara ihtiyaç olabileceği belirtilmektedir (Olumide S. vd. 2020). Ayrıca kötü niyetli kişilerin bu sistemleri kolaylıkla manipüle edebildiği tespit edilmiştir. Özellikle seçim sonuçlarını etkileyebilecek çift oy kullandırma, sayım sonucunu değiştirme gibi bazı durumların da ortaya çıkabilmektedir. Bu gibi durumların seçmenlerin dünya genelinde seçimin bütünlüğüne olan güvenini kaybetmesine neden olduğu bildirilmektedir (Chiang 2009).

2.2 Elektronik Oylama

Elektronik oylama (e-oylama) temel olarak geleneksel oylama sistemlerinde tanımlanan sorunları çözmek için tanıtılmıştır. E-oylama sistemi, seçim verilerinin dijital bilgi olarak kaydedildiği, saklandığı ve işlendiği bir oylama sistemidir. Genel olarak, bir e-oylama sistemi, seçim sürecine katılmak isteyen her vatandaş için elektronik cihazlar yardımıyla oylama imkânı sağlayan bir elektronik oylama ortamı sunmaktadır. Elektronik oylamanın geleneksel oylama yöntemine göre bazı avantajları olduğu belirtilmektedir. Bu tür sistemler, ilk olarak oy pusulalarının hızlı olarak toplanmasına ve sonuçların manuel oylama sistemine kıyasla daha kısa sürede hazırlanmasına olanak tanımaktadır. Geçersiz oy olasılığını azaltarak, oy kullanma ve sayma sürecindeki hata payını önemli ölçüde azaltacağı ön görülmektedir. Bu avantajlara ek olarak engelliler için gelişmiş erişilebilirlik ve oy pusulaları için çoklu dil desteği de sağlanabilmektedir (Sedky ve Ramzy Hamed 2015).

Temel olarak bir oylama sistemi kayıt, kimlik doğrulama, oy verme ve sayım aşamalarını içermelidir (Cranor ve Cytron 1997, Jardí-Cedó vd. 2012) Genel oy sistemi mimarisi Şekil 2.1'de gösterilmiştir.

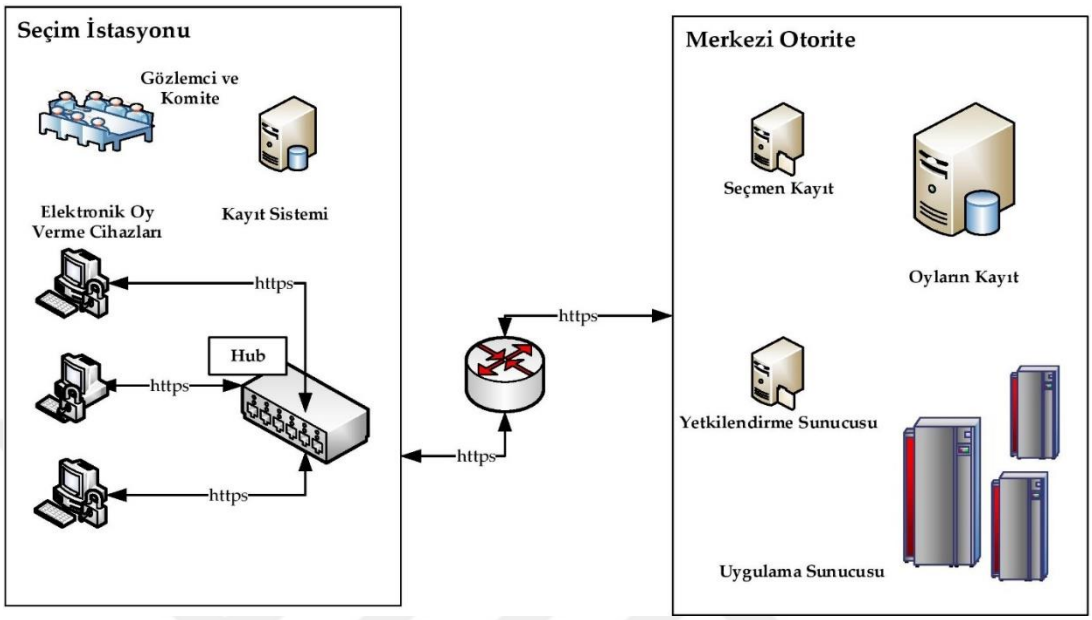
a) Kayıt (Registration); ilk süreç seçmen listelerin oluşturulması sürecidir. Bu aşamada oy vermeye yetkili kişilerin listeleri hazırlanmaktadır.

b) Kimlik doğrulama (Verification and Authentication); oy verme süreci için kimlik doğrulama kontrolü sürecidir. Doğrulamadan geçen kullanıcıya oy verme işlemi için izin verilir. Kimlik doğrulama için, seçmenlerin kimlik bilgileri oylama zamanından önce bir parola veya bir tür kimlik doğrulama belirteci kullanılarak doğrulanması beklenmektedir.

c) Oy verme (Casting); bu aşamada kimlik doğrulama işlemini başarı ile geçen kişiler oylarını kullanabilmektedir. Oyların gizliliği, anonimliği ve doğruluğu garanti edilmeli ve hiçbir şekilde değiştirilemez veya silinemez olması sağlanmalıdır.

d) Sayım (Counting); son olarak kullanılan oyların tasnif işlemleri yapılarak sonuçlar açıklanması sürecidir.

Klasik e-oylama uygulamalarında merkezi yetki kontrolü altında düzenlenerek sonuçlandırılmaktadır (Şekil 2.1). Bu tür sistemlerin çeşitli dezavantajları ve riskleri içerebilmektedir. Bunlardan başlıcaları; e-oylama sistemi standartlarının eksikliği, güvenlik ve güvenilirlikle ilgili riskler, bilgisayar korsanlığına karşı savunmasızlık, dolandırıcılığa açıklık, kötü amaçlı yazılım programlarının yüklenebilmesi ve işlemlerin güvenli depolanmaması olarak belirtilmektedir (Bishop ve Wagner 2007, Epstein 2007, Abuidris vd. 2019).



Şekil 2.1 Klasik Elektronik Oylama Şeması

Farklı amaçlar için kullanılan birçok farklı elektronik oylama sistemi mevcuttur. Bunlardan bazıları; Punç Kart (Punch Card), Doğrudan Elektronik Kayıt (Direct-Recording Electronic - DRE) (Fink vd. 2009), Halka açık ağlarda DRE (Public network DRE), Kiosk oylama (Gurubasavanna vd. 2019), mobil oylama (Khelifi vd. 2013) ve internet üzerinden (Oo ve Aung 2014, Tarasov ve Tewari 2017) oylama gibi sistemler mevcuttur.

DRE (Direct-Recording Electronic) oylama: Doğrudan Elektronik Kayıt makinesi, özel amaçlı oylama yazılımı çalıştıran özel olarak tasarlanmış elektronik cihazlardır. Bu sistemler, mevcut kâğıt tabanlı oylama sistemlerine benzerlik göstermektedir. Oylar, bir sandık yerinde bir oylama kabininde kullanılmaktadır, ancak kullanılan oylar elektronik sandıklara kaydedilmektedir. DRE sistemleri kolay kullanılabilirlik özellikleri sunabilmektedir. Özellikle çok dilli oy pusulalarının kullanımı, işitsel geri bildirim, ekrandaki büyütme özellikleri uygulanabilmektedir. Ayrıca çok sayıda aday içeren uzun oy pusulalarını kolaylıkla yönetilebilmektedir (Fink vd. 2009).

Kiosk oylama: Oylar DRE oylamasından farklı olarak oylama makineleri geleneksel oy verme yerlerinden uzakta, alışveriş merkezleri, kütüphaneler veya okullar gibi uygun yerlere yerleştirilmektedir. Oylama platformları yine de seçim görevlilerinin kontrolü altında olmakta ve fiziksel ortam gerektiğinde değiştirilip izlenebilmektedir. Tipik olarak, oy verme alanlarındaki oylama kabinleri elektronik oylama terminallerinden oluşmaktadır ve kapalı bir ağ üzerinden bağlanılmaktadır. Kullanılan oylar, elektronik sandıkların yerine bir sayım yetkilisi sunucusu tarafından kaydedilmektedir. Seçmenler, oylama kabinlerine girmelerine izin verilmeden önce kimlik doğrulaması yapılarak oy vermesine izin verilmektedir (Gurubasavanna vd. 2019).

Uzaktan Oylama: Bu tür sistemler mobil cihazlar veya internet üzerinden yapılan oylama sistemleri olarak tanımlanmaktadır. Çeşitli biyometrik kontrol sistemleri ile entegre edilerek, seçmenin istediği platformu kullanmasına imkân vermesi açısından dikkat çekmektedir (Gentles ve Sankaranarayanan 2012).

Elektronik sistemler devlet-vatandaş iletişiminin birçok evresinde çeşitli amaçlar (eğitim, nüfus, pasaport, tapu, sağlık vb.) için kullanılmaktadır. Elektronik oylama sistemlerinde bu hizmetler arasına girmeye başlamıştır. Elektronik oylama sisteminin ilk kullanımı ise ABD'de 2000 yılında gerçekleşmiştir. Bunu Fransa (2001), İngiltere (2002), İspanya (2003), İrlanda (2004), Estonya (2005), Portekiz (2005), Hollanda (2004, 2006, 2007), Paraguay (2008), Finlandiya (2008), Avusturya (2009), Almanya (2009), Norveç (2011) izlemiştir. Estonya, 2005'teki küçük çaplı bir seçim sırasında elektronik oylama sistemini kullanılmasının ardından, 2007 yılında ulusal parlamento seçimlerinde de uzaktan elektronik oylamaya izin veren ilk ülke olmuştur (Esteve vd. 2012).

2.2.1 Elektronik seçim sistemin özellikleri

Elektronik oylama sistemlerinde aşağıdaki özelliklerin yer alması gerektiği belirtilmektedir. Bunlar;

a) *Belge Serbestliği (Receipt-Freeness),* seçmenin belirli bir aday için seçimini yaptığını kanıtlamak için herhangi bir belge sunmamalıdır (Ali ve Murray 2016).

b) *Adalet (Fairness), Şeffaflık (Transparency)* Diğer seçmenlerin kararlarını etkileyen ön sonuçlara ulaşılmamalıdır. Şeffaflık ilke olarak seçimi gözlemlenebilir hale getirerek gerçekleştirilmelidir. Bağımsız üçüncü tarafların seçim süreçlerini gözlemlemesine ve incelemesine izin verilerek sağlanmalıdır. Gözlemciler seçim süreçlerine asla müdahale etmemeli, ancak yine de seçimi inceleme ve doğrulama imkânına sahip olmalıdır (Fujioka vd. 1993, Anane vd. 2007).

c) *Veri Bütünlüğü (Data Integrity)* her oylamanın amaçlandığı gibi kaydedilmesini ve kaydedildikten sonra hiçbir şekilde değiştirilememesini sağlamalıdır (Keshk ve Abdul-Kader 2007). Aynı zamanda hiçbir oyun sayımı öncesinde, sırasında veya sonrasında değiştirilemez olması sağlanmalıdır.

d) *Mahremiyet / Seçmen Anonimliği* (*Privacy / Voter Anonymity*) Seçmenlerin kimlikleri ve kime oy verdikleri açıklanmamalıdır (Anane vd. 2007). İlke olarak oy gizliliği, hiçbir seçmenin bir oyla ilişkilendirilemeyeceğinin güvencesini içermelidir.

e) *Uygunluk (Eligibility)* sadece kayıtlı seçmenlerin oy kullanmasına izin verilmelidir (W. Zhang vd. 2018).

f) *Güvenilirlik / Sağlamlık* (*Reliability / Robustness)* seçim sistemleri oy kaybı olmadan güvenli bir şekilde işlemelidir. Sistemler saldırılara karşı dirençli olmalı, herhangi bir kötü amaçlı kod ve hata içermeyecek şekilde tasarlanmalıdır (Ryan vd. 2009).

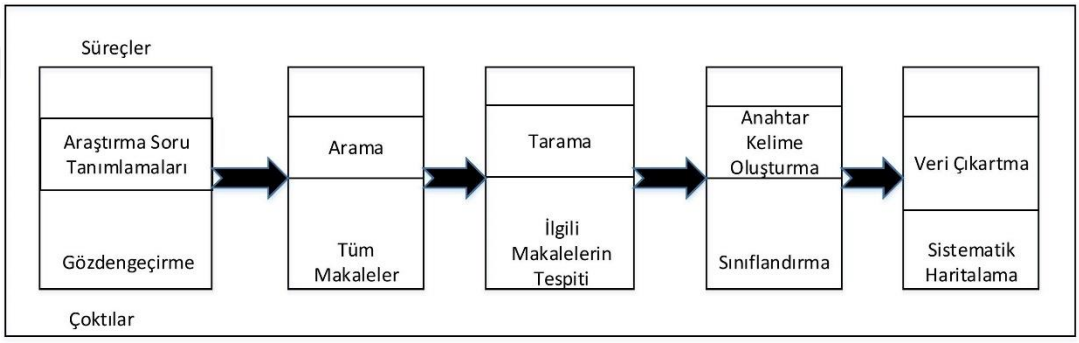
g) *Benzersizlik (Uniqueness)* seçmenlerin birden fazla oy kullanmasına izin verilmemelidir (Sun vd. 2019, Bokslag ve de Vries 2016).

h) *Doğrulanabilirlik (Verifiability)* oylar düzgün sayıldığı garanti altına alınmalı ve sayımının doğrulanabilir olmalıdır (Liu ve Wang 2017).

Özellikle blok zinciri yapısının şeffaf ve verilerin değiştirilemez olduğu kabul edilmektedir. Bu sebeple blok zinciri sistemlerinin elektronik oylamalardaki şeffaflık ve veri bütünlüğü özelliklerine katkı sağlayacağı düşünülmektedir.

3. LİTERATÜR DEĞERLENDİRMESİ

Tez çalışmasında öncelikle elektronik oylamalardaki eksiklikler incelenmiştir. Blok zinciri sistemlerinin yer aldığı literatür taramasında Petersen ve arkadaşlarının önerdiği sistematik haritalama yöntemi izlenerek literatür taraması yapılmıştır (Petersen vd. 2008). Bu yöntem araştırma sorularının belirlenmesi, arama, tarama, sınıflandırma ve veri çıkartma aşamalarını içermektedir (Şekil 3.1).



Şekil 3.1 Sistematik Haritalama Yöntemi

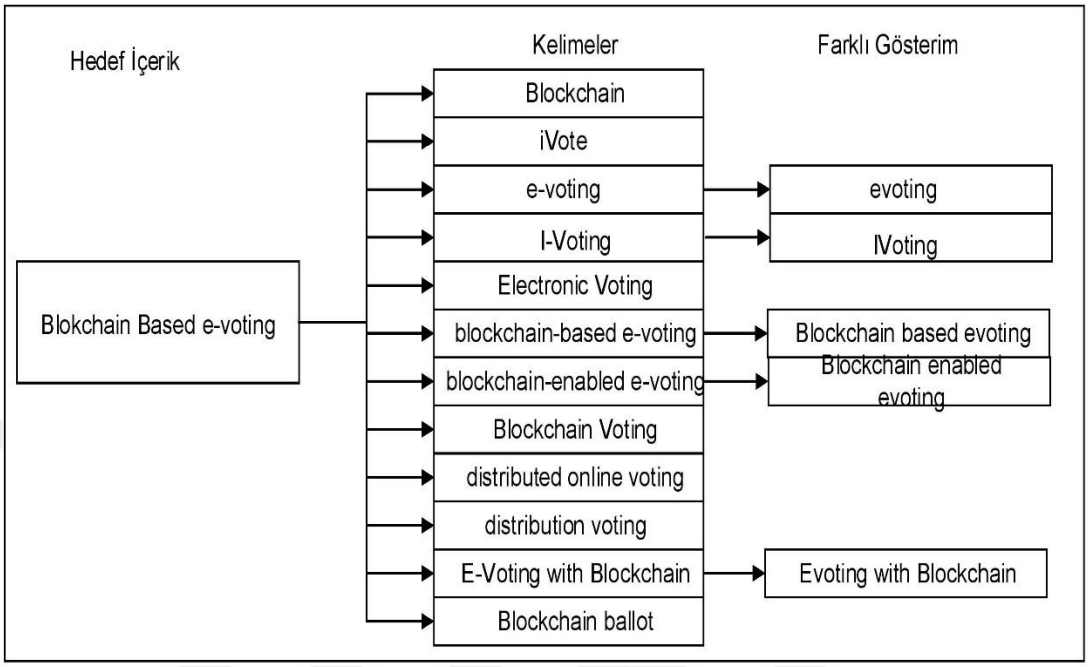
Blok zinciri oylama sistemlerinin yer aldığı literatür taramasında öncelikle araştırma soruları belirlenmiştir, belirlenen sorulara cevaplar araştırılmıştır.

a) Blok zinciri elektronik oylama sistemleri,

b) Blok zinciri sisteminin katkıları,

c) En çok tercih edilen blok zinciri altyapısı nelerdir.

Öncelikle literatür incelemesinde yer alacak makalelerin tespit edilebilmesi amaçlanmıştır. Bu sebeple yapılan arama sonuçlarının anlamlı olabilmesi için sorgu kelimelerinin tespiti yapılmıştır (Şekil 3.2). Tarama yapılan bilimsel veri tabanların da aynı arama kriterleri uygulanarak sonuçlar elde edilmiştir.



Şekil 3.2 Sorgu Kriterleri

Arama dizesi ile aşağıda belirtilen çevrimiçi veri tabanlarından tarama işleme yapılmıştır. Bu kriterlere göre makaleler belirlenmiştir.

a) IEEE Xplore,

b) Arxiv,

c) Iacr,

d) ScienceDirect,

e) Web of Science,

f) Scitepress,

g) Springer,

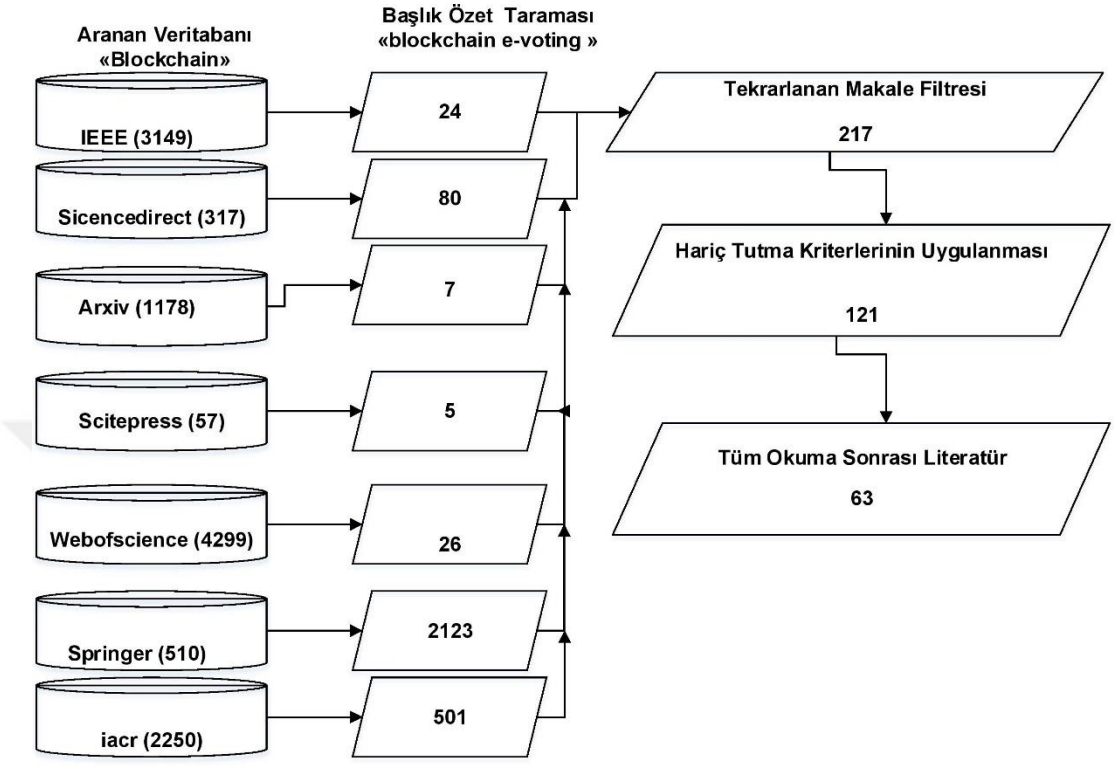
Daha sonra, tespit edilen makalelerden dâhil etme ve hariç tutma kriterlerine göre tasnif edilmesi işlemi uygulanmıştır. Bu aşamada, makalelerin İngilizce olarak hakemli bir dergide yayınlanmış olanlar arasından, odakları blok zinciri tabanlı e-

oylama sistemleri olarak yer alanlar incelemeye dâhil edilmiştir. Diğer dillerde yayınlanan makaleler ile farklı alanlarda (örneğin sağlık, finans vb.) blok zinciri kullanımını inceleyen makaleler hariç tutulmuştur. Makale seçim süreci diyagramı Şekil 3.3'te verilmiştir. Bazı makallerin farklı veri tabanlarında da olduğu görülmüştür. Bu tür mükerrer makaleler elendikten sonra, makaleler başlıklarına ve özetlerine göre incelenmiştir. Araştırma konusu ile ilgili olmayan makaleler elenmiştir. Veri tabanlarından elde edilen sonuçlarda bazı durumlar için beklenmedik sonuçlar da elde edilmiştir. Web of Science, Scitepress ve Springer veri tabanları farklı arama algoritmaları kullandığı için makale sayısı beklediğimizden fazla çıkmıştır (Çizelge 3.1).

Çizelge 3.1 Bilimsel makale sorgu sonuçları

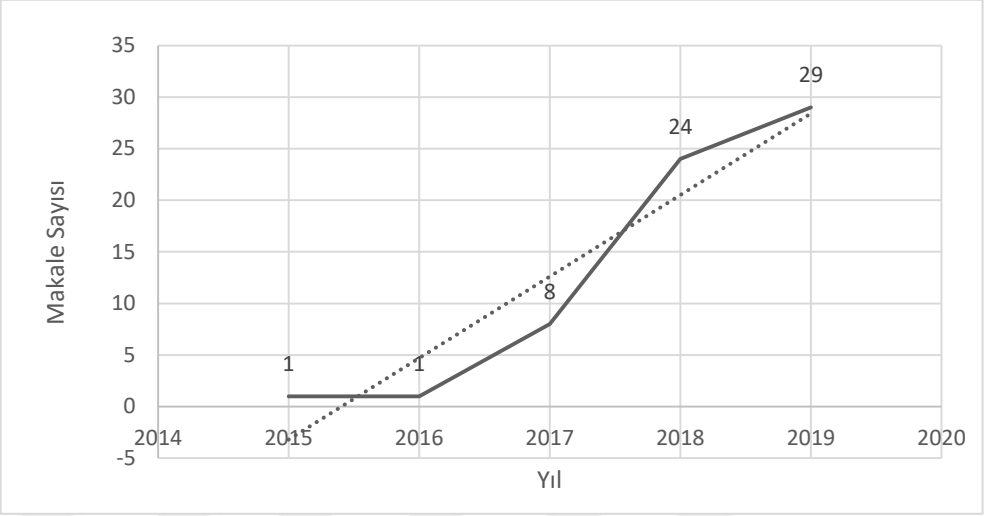
Bilimsel Makale Veri tabanı	**Blockchain**	**E-voting**	**Blockchain Ballot**
sciencedirect.com (Future Gen. Comp. Sys, Comp. & Sec., Journal of Network and Comp. App. Procedia Comp. Science)	317	462	80
arxiv.org	1178	56	7
ieeexplore.ieee.org (conferences and journals)	3149	290	24
scitepress.org	57	100	5
webofscience.com	4299	740	26
springer.com (journal)	510	2123	2126

Ancak, bu sonuçlar istenen arama sonuçlarını olumsuz etkilememiştir. Şekil 3.4 seçilen makalelerin yayın yılı dağılımını göstermektedir. İlginç bir şekilde, seçilen tüm makalelerin 2014 yılından sonra yayınlandığı görülmüştür. Bu durum 2009 yılında Bitcoin ile başlayan blok zinciri uygulama alanının e-oylama alanında yeni olduğunu göstermektedir.



Şekil 3.3 Makale seçim süreci diyagramı

Makaleler yayın yılına göre incelendiğinde 2017 yılında 8 (% 12,69), 2018 yılında 24 (% 38,09) ve 2019 yılında 29 (% 46,03) makalenin bu veri tabanlarında yer aldığı tespit edilmiştir. Bu sonuç blok zinciri oylama araştırmalarının her yıl hızla arttığını göstermiştir.



Şekil 3.4 Araştırma yayın trendi

3.1 Elektronik Oylamadaki Eksiklikler

Elektronik oylama sistemlerini özellikle operasyonel maliyet, daha az insan hatası ve daha hızlı sonuçların elde edilebilmesi nedeniyle geleneksel oylama sistemlerine göre bazı avantajlara sahip olduğu belirtilmektedir. Çevrimiçi oy verme gelişmelerinin özellikle yaşlıların, engellilerin ve isteksiz gençlerin erişilebilirliğini kolaylaştırması nedeniyle seçmen katılımını artırabileceği belirtilmektedir. Ayrıca uzaktan erişimli elektronik oylama sistemleri yardımıyla da lokasyon bağımsız katılım sağlanabileceği ön görülmektedir. Oy pusulalarının basılması, dağıtımı ve sayımı gibi maliyetler konusunda da elektronik oylama sistemlerinin düşük maliyetli olabileceği belirtilmektedir (Bokslag ve de Vries, 2016). Bununla birlikte, elektronik oylama sistemlerinde potansiyel dezavantajlar olabileceği de ortaya çıkmıştır. E-oylama sistemlerinin yazılım, donanım ve iletişim altyapısı gibi birçok farklı sistemin entegrasyonunu gerektirmesindeki zorluklar sebebiyle, kullanılan sistemlerde bazı güvenlik zafiyetleri ortaya çıkabilmektedir. Bunlardan kimlik hırsızlığı en önemli tehditlerden birisidir. Casus yazılımlar, virüsler, solucanlar, sunucu sızma saldırıları, sahtekârlık, sahte web sayfaları, DNS (Etki Alanı Adı Sunucusu) saldırısı ve DDoS saldırısı (Dağıtılmış Hizmet Reddi- Distributed Denial of Service) gibi farklı türlerde

saldırılarla da karşı karşıya kalabilmektedir. Dijital sistemlerde içeriden gelebilecek saldırıların da potansiyel sorunlar arasında olduğu belirtilmektedir (Noizat 2015).

Genellikle merkezi bir yapı üzerinde tasarlanan elektronik oylama sistemleri, DDoS saldırısı gibi siber saldırı türlerine açık olmaktadır. Bu tür bir saldırı, sistemlerin çalışmasını yavaşlatabilmektedir. Bu tür bir saldırı neticesinde bazı durumlarda sistem çalışamaz hale gelebilmektedir. Sistem kullanılabilirliği, gizlilik veya kimlik doğrulama sorunları ortaya çıkabilmektedir (Bokslag ve de Vries 2016). Verilerin uzak sunuculardaki saklanmasının verilerin yedekliliği açısından avantajlı olduğu varsayılmaktadır. Ancak bu durumun da bilgisayar korsanlarının saldırılarına karşı riskler barındırdığı, hatta sistem güvenliği yönetiminin zayıf olması durumunda veri kaybına veya hasarına neden olabileceği belirtilmektedir. Ayrıca, geleneksel veri tabanları tek bir grup veya merkez tarafından yönetilmektedir. Yetkili kişilerin depolanan kayıtlara erişebilir olması, veri tabanı üzerinde kapsamlı bir kontrole sahip olması bazı veri güvenliği risklerine sebep olabileceği değerlendirilmektedir. Ayrıca, kullanılan yazılım ve donanımlardaki tespit edilemeyen güvenlik zafiyetleri sebebiyle öngörülemeyen saldırılara açık hale gelebilmektedir. Örneğin ortadaki adam saldırısının (Man in the Middle) bunlardan biri olduğu belirtilmektedir (Cardillo ve Essex 2018). Güvenilmeyen istemci cihazları da (telefonlar, bilgisayarlar, dizüstü bilgisayarlar) kendilerine özgü açıklıkları içerebilmektedir. Benzer saldırılar için farklı bir alan oluşturmaktadır. Herhangi bir açıklık barındıran bu tür cihazlar, çevrimiçi oylama sırasında saldırganlara bir şekilde seçmenlerin kimlik doğrulama bilgilerini elde etme ve verileri değiştirebilme ihtimali sunmaktadır. Sunucu sistemleri de sistemi çalışmaz hale getirilmek amacıyla benzer saldırıların hedefi olarak ortaya çıkabilmektedir. Ayrıca, oy pusulaları elektronik olarak iletildiği için, manipüle edilmiş olarak gelen bilginin sisteme kayıt edilmesi durumunda bu verilerin doğruluğunu tespit etmek zor olmaktadır. Bu nedenle güvenlik ve oy değiştirme riski, elektronik bir oylama sistemindeki kritik engeller olarak hala gündemde yer almaktadır. Özellikle farklı altyapı ve yeni oylama yöntemleri söz konusu olduğunda

kullanılan cihazlardaki ve sistem altyapısındaki tehlikeleri önceden belirleme imkânı olmamaktadır (Susskind 2017).

Saldırıya uğramış çeşitli seçim yazılımları veya sistem örnekleri mevcuttur. Bu saldırılar da, özellikle operasyon sırasında çevrimiçi bir oylama ağının kolayca bozulabildiği gösterilmiştir (Oo ve Aung 2014, Luo vd. 2018). Genellikle bu tür elektronik oylama sistemlerindeki oylama süreçleri şeffaf değildir (Bokslag ve de Vries, 2016). Günümüzde kullanılan elektronik oylama sistemleri özel olarak tasarlanmış ve merkezileştirilmiştir. Sistemin geliştirme kodları, veri tabanı, sistemi kontrol eden yazılımlar, izleme araçlarının kurulumu için merkezi bir tedarikçi kullanılabilmektedir. Bu sistemlerde kullanılan oylama yazılımları genellikle halkın erişimine açık olmadığından, yazılımı kontrol eden kişiler tarafından manipüle edilebileceğine dair şüpheyle yaklaşılmasına sebep olmaktadır (Noizat 2015). Bağımsız olarak doğrulanabilir kontrol mekanizmasının olmaması, merkezi sistemlerin seçmenlerin ve seçim organizatörlerinin ihtiyaç duyduğu güvenilirliği elde etmesini zorlaştırmaktadır. Bir başka sorun da, uzaktan oylama sistemini kullanan yapılarda, seçmenin zorla belirli bir adaya oy vermesinin zorlanması durumunda da bazı problemlerin olabileceği belirtilmektedir (Shahzad ve Crowcroft 2019).

Bağımsız birimler tarafından sayımın ve sonuçların çapraz kontrollerinin sağlanabildiği bir mekanizma kurmanın önemli olduğu belirtilmektedir. Bu amaçla, seçim sonuçlarının doğruluğunu kontrol etmek için risk sınırlayıcı denetimler önerilmektedir. İstatistik yöntemlerle hesaplanan sonuçlarda bulunan hatalar dikkate alınarak, yanlış sonuçlar için güçlü kanıtlar elde edildiği belirtilmektedir (Bernhard vd. 2017). Elektronik seçimlerdeki başarısız uygulamalar motivasyon kaybına neden olmaktadır (Palas Nogueira ve de Sá-Soares 2012). Bu sonuçlardan dolayı, hükümetler ve seçmenler tarafından elektronik oylama sistemlerine güven kriterleri her zaman ön planda yer almakta ve genellikle zayıf olarak kategorize edilmektedir (Achieng ve Ruhode 2013). Son yıllarda geliştirilen iki büyük e-oylama uygulamasın da benzer şekilde büyük güvenlik riskleri içerdiği belirlenmiştir. 2015'teki Virginia

seçimlerinden sonra, Virginia Bilgi Teknolojileri Ajansı (VITA - Virginia Information Technologies Agency), e-oylama sisteminin çeşitli bölümlerine güvenlik testlerini uygulamışlardır. Fiziksel ağ, işletim sistemi, veriler ve oy verme süreçlerini test etmişlerdir. VITA, sistemde güvenli olmayan güvenlik protokollerinin ve zayıf parolaların kullanıldığını belirlemişlerdir. Ayrıca, saldırganın verilerin gizliliğini ve bütünlüğünü tehlikeye atabildiklerini ortaya çıkarmışlardır. Bu sorunlar nedeniyle, Gelişmiş Oylama Sisteminin kullanımına son verilmesi tavsiye edilmiştir (Annoymous 2015). Başka bir örnekte ise, İsviçre hükümeti ülkede e-oylama sisteminin uygulanması için uzun yıllar özel sektörle birlikte çalışmıştır. Swiss Post bu konu üzerinde çalıştıktan sonra uygulamaların güvenirliliğine ve şeffaflığına inandıkları için, uygulamalarını 2019'da güvenlik testleri için herkese açmışlardır. Uluslararası siber güvenlik uzmanları, Swiss Post uygulamasının kaynak kodunda uygulanan karıştırma yönteminde kritik bir hata sonucunda oylamada manipülasyon yapılabilen bir açıklık tespit etmişlerdir. Bu açıklık yardımıyla, bilgisayar korsanlarının geçerli oyları sahte oylarla değiştirebildiklerini göstermişlerdir (Lewis vd. 2019, Stone 2019). Bu kritik sorunların sonucu olarak İsviçre Hükümeti sistemin kullanımını iptal etmiştir.

Yang ve arkadaşlarının 2018 yılında yaptıkları çalışmada, ABD, Hindistan ve Brezilya gibi ülkelerdeki son çevrimiçi oylama deneyimlerini incelemişlerdir. Çevrimiçi oylama sistemlerinin gelecek seçimler için güvenlik seviyelerini iyileştirmek, oyların gizliliğini sağlamak, bütünlüklerinin ve geçerliliklerinin doğrulanmasını sağlamak için daha fazla araştırmaya ihtiyaç olduğunu belirtmişlerdir (Yang vd. 2018).

Son birkaç yılda önerilen blok zinciri tabanlı e-oylama yöntemlerine yönelik bazı eleştiriler de yayınlanmaya başlamıştır. Örneğin; MIT (Massachusetts Institute of Technology) uzmanları, Batı Virginia'da 2018 ara seçimleri sırasında kullanılan bir mobil oylama uygulamasında meydana gelen güvenlik açığını tespit etmişlerdir (Specter vd. 2020). Bu güvenlik açığının, bilgisayar korsanlarının oyları değiştirmesine olanak tanıdığı vurgulanmıştır. Bazı araştırmacılar, blok zinciri

sistemlerin maruz kalabileceği başka güvenlik açıklarını da getirebileceğini belirtmişlerdir (Bollinger ve McRobbie 2018). Örneğin akıllı sözleşmelerdeki güvenlik açıkları veya % 51 saldırısı, bu tür sistemler için teorik olarak iyi bilinen potansiyel bir tehdit olduğu belirtilmiştir. Ayrıca, kötü niyetli madencilerde, öğelerin eklendiği işlemleri kontrol edebilmeleri açısından tehdit unsuru olarak değerlendirmesi gerektiğine dikkat çekilmiştir (Juels vd. 2018, Goodman ve Halderman 2020, S. Park vd. 2020). Son olarak çevrimiçi oylamalardaki riskler kriptografik ve yapılandırma hataları, altyapı sorunları, web veya mobil uygulama açıklıkları olarak ortaya çıkabilmektedir (Bull vd. 2018).

3.2 Blok Zinciri Tabanlı Elektronik Oylama Sistemleri

Çalışmanın bu bölümünde, blok zinciri teknolojisinin güvenli bir elektronik oylama sistemi için yapılan çalışmalar incelenmiş olup, incelenen makaleler 5 ana gruba ayrılarak değerlendirilmiştir. Bu kategoriler, blok zincirinin uygulanabilirliğini öne çıkaran genel öneriler, farklı kripto para birimi ve altyapılarını kullanan sistemler, gizlilik konusunda yapılan çalışmalar, farklı fikir birliği kullanımı ve veri bütünlüğünü öne çıkaran araştırmalar olarak ele alınmıştır.

a) Genel: Araştırmacılar mevcut çevrimiçi oylama sistemlerine alternatif olarak blok zinciri teknolojisinin, seçmenlerin güvenini sağlayabileceğini belirtmişlerdir. Blok zinciri kullanan çevrimiçi uygulamalarını hükümetlerin benimseyebileceği bir çözüm olabileceği sonucuna vardıklarını belirtmişlerdir. Birçok araştırmacı, blok zinciri platformunda akıllı sözleşmeleri kullanmanın, e-oylamaya önemli bir katkı sağlayacağına dikkat çekmektedir (Sudharsan vd. 2019). Bu tür sistemlerin maliyet verimliliği sağladığı ve elektronik oylama sistemlerinin ölçeklenebilirliğindeki sınırlamaların üstesinden gelmek için yeni olanaklar sunduğu vurgulanmıştır (Riemann ve Grumbach 2017, Dricot ve Pereira 2018, Schiedermeier vd. 2019). Genellikle blok zincirinin güvenlik ve şeffaflık gereksinimleri ile karmaşık uygulamaları desteklemede, uygun bir çözüm olarak düşünülebileceği vurgulanmıştır (Heiberg vd. 2018, Srivastava vd. 2018, Bosri vd. 2019, Q. Zhang vd. 2019). Kshetri

ve arkadaşlarının önerdiği yapıda öncelikle oy kullanmaya yetkili kişilere para dağıtılmakta daha sonra sadece bir kez harcama yapmalarına izin verilerek oylama yapılabileceği belirtilmiştir (Kshetri ve Voas 2018). Hardwick ve arkadaşları tarafından önerilen sistemin farkı ise; diğer sistemlerdeki gibi merkezi olmayan planlamanın yanı sıra oylama döneminde seçmenlerin oylarını değiştirmelerine ve güncellemelerine imkân vermesi olarak belirtilmektedir. Ancak, gizlilik, tutarlılık ve denetlenebilirlilik konusu ele alınmamıştır (Hardwick vd. 2018).

Sadia ve arkadaşları, Shahzad ve Crowcroft, Teja ve arkadaşları gibi bazı araştırmacılar yine blok zincirinin genel avantajlarına ek olarak blok zinciri tabanlı güvenli e-oylama modelinde özellikle akıllı sözleşmeler kullanmanın önemini ve faydalarını vurgulamışlardır. Akıllı sözleşmelerin üçüncü parti çözümlerle birlikte uygulandığı takdirde blok zinciri özelliklerinin kullanımını basitleştirdiği öne çıkarılmıştır (Sadia vd. 2019, Shahzad ve Crowcroft 2019, Teja vd. 2019). Na ve arkadaşları blok zinciri alt yapısını kullanan web tabanlı blok zinciri altyapısını kullanan bir oylama sistemi önermişlerdir (Na ve Park 2018). Sohbet özelliği de olan uygulamalarında anonimlik sağlanabilmektedir. Aynı zamanda oy kullanabilme imkânı da sunulmuştur. Ayrıca son zamanlarda yapılan bazı çalışmalarda, bulut tabanlı hizmetlerin artmasıyla birlikte bulut ortamında da blok zinciri tabanlı e-oylama tasarlanması önerileri de yapılmıştır. Bulut çözümlerinin hizmetlere kolay erişim, üstün hizmet performansı ve maliyet avantajları sağladığı belirtilmiştir (Bellini vd. 2019, Sathya vd. 2019).

Blok zinciri entegrasyonu nedeniyle olası teknik veya kullanıcıyla ilgili sorunlara da odaklanan çalışmalar da yayınlanmıştır. Khan ve arkadaşları işlemlerin aynı anda yürütüldüğü sırada ana düğümde artan bir iş yükü oluştuğu takdirde, blok zincirinde gecikmiş işlemlerin gerçekleşebileceği sonucuna varmışlardır (Khan vd. 2020). Öte yandan Johnson seçmenlerin dijital okuryazarlığının, seçmenlerin teknik bilgisinin veya sistemin ölçeklenebilirliğinin eksikliği gibi konuların blok zinciri tabanlı e-oylamanın potansiyel risklere sahip olduğuna dikkat çekmiştir (Johnson 2019).

b) Kripto para tabanlı çözümler: Blok zinciri tabanlı kripto para birimlerinin kullanılmasının ardından, bu tür sistemlerin altında yatan yeniliklerden birinin de farklı ihtiyaçlar içinde kullanılabileceğin anlaşılmaya başlanması olmuştur (Zhao ve Chan 2016). Bu doğrultuda Bitcoin tabanlı bir e-oylama sisteminin, bireysel oyların mahremiyetini korumaya yardımcı olacağı belirtilmiştir (Zhao ve Chan 2016, Bao vd. 2018). Zhao ve Chan'ın çözümlerinde sıfır bilgi kanıtı (Zero knowledge proof) kriptografi yönteminin kullanılmasını önermiştir. Bu sayede seçmen ve oyu arasındaki ilişkinin gizlenmesi hedeflenmiştir (Zhao ve Chan 2016). Bitcoin 'den farklı olarak literatürde birçok Ethereum tabanlı e-oylama platformu, elektronik oylama sistemlerinde denenerek uygulama alanları araştırılmıştır (Q. Zhang vd. 2019, Shukla vd. 2018). Ethereum çerçevesinin hem özel hem de genel ağlarda oluşturulması imkânı olduğu belirtilmektedir. Akıllı sözleşmelerin ve dağıtılmış uygulamaların etkinleştirilmesine yardımcı olması sebebiyle de ilgi çekmektedir (Lai vd. 2018, Yavuz vd. 2018, X. Fan vd. 2020).

Bartolucci ve arkadaşları uygulamalarına daire karıştırma tekniğini (circle shuffle) eklemiştir. Ancak bu teknik, merkezi bir kontrol otoritesi gerektirmektedir. Güvenilir bir otorite olsa dahi kötüye kullanma potansiyeline sahipse, tüm oylama protokolü açısından riskli olabilmektedir. Bu protokolün konuşlandırılması, seçmenlerin ve oy pusulalarının bağlantısının ayrışmasına yardımcı olduğu belirtilmiştir (Bartolucci vd. 2018).

Thuy ve arkadaşları Votereum adını verdikleri blok zinciri oylama sistemini tasarlamışlardır. Oylama işlemlerinin uygulanmasın da seçmenlerin mahremiyetini ve güvenliğini sağlayacağı belirtilmiştir. Sistemlerinin sağlamlık, gizlilik, doğrulanabilirlilik gibi temel gereksinimleri desteklediği için seçimlerde kullanılabileceği belirtilmiştir. Ancak bu sistemin makbuzsuz olduğunu teyit etme ve baskıya direnme yeteneğine sahip olmadığını belirtmişlerdir (Thuy vd. 2019). Hjalmarsson vd. ve Teja vd. blok zinciri ile geliştirilen sistemlerin de seçmenlerin ve otoritenin tüm işlemlerin güvenli, uygun maliyetli ve şeffaf olmasının sağlanabileceği sonucunu belirtmişlerdir (Hjálmarsson vd. 2018, Teja vd. 2019). Yavuz ve

arkadaşları Android platformu üzerinde akıllı sözleşme kullanarak Ethereum altyapısını kullanan oylama uygulamasını geliştirmişlerdir. Ancak temel dezavantajları sağlamlık ve makbuz serbestliği özelliklerini desteklemiyor olması olarak ortaya çıkmıştır (Yavuz vd. 2018).

Blok zinciri kapsamında benimsenen bir diğer platform ise Hyperledger'dır. (Yu vd. 2018). Hyperledger, özel veya izin tabanlı bir ağ yapısı şeklinde tasarlanabilmektedir. Tasarım gereksinimlerine göre, hem iş süreçleri hem de belirteçler için zincir kodu (chaincode) adı verilen özel geliştirme ortamı ile geliştirilen uygulamalarla kullanılabilmektedir. Zincir kodu, ağ üyeleri tarafından kabul edilen iş mantığını işlediği için akıllı sözleşmelere benzer bir programdır. Bu sistemlerin geliştirme ortamı olarak kullanıldığı sistemlerde performansı, ölçeklenebilirliği ve gizliliği artırmaya yardımcı olabileceği iddia edilmiştir. Yazarlar Zhang ve arkadaşları uçtan uca gizliliği korumak için Hyperledger platformunu kullanan oylama sistemini önermişlerdir. Ancak sistemlerinin doğrulanabilirlilik ve tutarlılık sağlamadığı belirtilmiştir (W. Zhang vd. 2018).

Zcash, halka açık başka bir kripto para birimi olarak kullanılmaktadır. İşlem verilerini halka açık olarak dağıtmaktadır. Zcash, Bitcoin ‘in aksine gizlilik sağlamaktadır. Tarasov ve Tewari bu çözümü elektronik oylama sisteminde blok zinciri altyapısı olarak önermişlerdir. İşlemlerde anonimlik sağlamanın yanı sıra seçimin güvenli ve şeffaf olmasını sağlandığı belirtilmiştir. Temel protokol özeliklerinde herhangi bir özelliğinde değişiklik uygulanmamış sadece; oylama protokolü alternatif bir kullanım durumu olarak sunmuşlardır. Sistemlerinin zorlamaya dirençli olmadığını belirtmişlerdir (Tarasov ve Tewari 2017).

Sun ve arkadaşları Quantum blok zincirini kullanan alternatif bir alt yapı önermişlerdir. Quantum blok zincirinin elektronik oylama süreçlerini basitleştirdiği sonucuna varmışlardır. Güvenli iletişimin kuantum bağlayıcı özelliği nedeniyle, seçmenlere sunulan oy pusulalarının değiştirilemez olduğu belirtilmiştir. Bu nedenle

adalet ve anonimlik sağlandığı belirtilmiştir. En büyük dezavantajının, denetlenebilirlilik tutarlılığını sunmaması olarak öne çıkmıştır (X. Sun vd. 2019).

Srivastava ve arkadaşları makalelerinde blok zinciri kullanan seçim sistemlerinde bulunan ölçeklenebilirlik ve güvenlik sorunlarını ele almışlardır. Standart blok zinciri protokolünü kullanmak yerine phantom protokolünü kullanmışlardır. Bu yöntemin ölçeklenebilirlik ve güvenlik sorunlarına çözüm sağlarken aynı zamanda hızlı bir oylama süreci de sağladığını belirtmişlerdir (Srivastava vd. 2018). Öte yandan, Lai ve Wu, seçmenlerin otoriteye veya hükümete olan güvenini en üst düzeye çıkarmak için merkezi olmayan ve anonim blok zinciri tabanlı bir e-oylama sistemi tasarlamak için Ethereum blok zincirini kullanmışlardır. Bu sayede seçimlere şeffaflık kazandırılacağını belirtmişlerdir. (Lai vd. 2018)

c) Gizlilik: Bu araştırmalarda yeni kriptografik prosedürlerin ve protokole dayalı çözümlerin uyarlanmasının gizliliği artırabileceği ve makbuz özgürlüğüne kavuşabileceğini öne süren argümanlar sıklıkla vurgulanmıştır. 2019 yılında yapılan iki çalışma da Çin Kalan Teoremi (Chinese Remainder Theorem) (Tso vd. 2019), bağlanabilir halka imzası (linkable ring signature) yöntemlerinin oylama çözümlerin bir uyarlamasını tasarlanmıştır ve gizliliğin sağlanabildiği belirtilmiştir (Lyu vd. 2019).

Araştırmacılar bu teoremlerden farklı olarak anonimliği ve gizliliği sağlamak için çeşitli algoritmaları da test etmişlerdir. Bunlardan bazıları homomorfik şifreleme (Dagher vd. 2018, Lee vd. 2019), halka imzası (ring signature) (Mercer, 2016, Liu ve Wang, 2017, Lai vd. 2018), blind signature (Liu ve Wang 2017, Chaieb vd. 2019), etkileşimli olmayan sıfır bilgi kanıtları (non-interactive zero-knowledge proofs) (Matile vd. 2019, Murtaza vd. 2019), çok seviyeli çoklu gizli paylaşım (multi-level multi-secret sharing) (J. Li vd. 2019) ve eliptik eğri kriptografisi (Tso vd. 2019, Dimitriou, 2019) olarak sıralanabilmektedir.

Liu ve Wang ’un 2017 yılında yaptıkları çalışmada güvenilir üçüncü taraflar olmadan bir blok zinciri oylama planı sunmayı hedeflemişlerdir. Önerdikleri sistemde

şeffaflık, doğrulanabilirlilik, tutarlılık, denetlenebilirlilik ve anonimlik sağlayan, bir yapı önermişlerdir. Araştırmacılar sistemlerinde seçim sırasında seçmenlerin tercihlerini korumak için kör imza (blind signature) kullanmışlardır (Liu ve Wang 2017). 2018 yılında Wang ve arkadaşları makbuz özelliklerini, tek seferlik halka imzasını ve homomorfik şifreleme yöntemini kullanan büyük ölçekli bir oylama sistemini önermişlerdir. Sistemlerinde akıllı sözleşme tabanlı Ethereum yapısı uygulayarak blok zinciri tabanlı oylama sistemlerinin güvenliğini ve anonimliği korumak için homomorfik ElGamal şifreleme yöntemini ve halka imzasını kullanmak üzere tasarlamışlardır. Ancak sistemlerinin zorlama direnci sağlamlığını desteklemediği belirtilmiştir (Wang vd. 2018). Shahzad ve Crowcroft (Shahzad ve Crowcroft 2019) verileri güvenceye almak için daha etkili bir hibrid teknik kullanarak bloklar oluşturmak ve mühürlemek için benzer bir çerçeve önermiştir. Blok içindeki işlem çifti bir özet fonksiyonu işlemine tabi tutulmuştur, özet fonksiyonunun ekstra kullanımı matematiksel karmaşıklığı arttırdığını göstermişlerdir (Bartolucci vd. 2018, Fusco vd. 2018). Bu tür dağıtılmış veri şifreleme tekniklerini, depolama verimliliğini artırmak önermişlerdir.

Murtaza ve arkadaşları Sıfır Bilgi Özlü Etkileşimli Olmayan Bilgi Argümanı (zkSNARKs Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) kullanarak seçmenlerin anonimliğini garanti eden blok zinciri tabanlı bir e-oylama sistemi önermiştir. Sistemde kimlik doğrulama sağlamak için dijital imzalar kullanılmıştır, ancak katılımcılarla herhangi bir etkileşim kullanılmamıştır (Murtaza vd. 2019). Chaieb ve arkadaşları Oyunuzu Doğrulayın (Verify Your Vote) adlı güvenli bir çevrimiçi oylama sistemi tasarlamışlardır. Protokollerin doğrulanabilirlilik, adalet, oy gizliliği, makbuz serbestliği vaat edilirken anonimliği desteklemediği belirtilmiştir (Chaieb vd. 2019).

d) Veri Bütünlüğü: Bütünlük, dikkate alınması gereken en önemli kriterlerdendir. Bu kapsamda veri aktarımının ve veri depolanmasının güvence altına alınması önemlidir. Dağıtılmış Veri tabanı Yönetim Sistemi (DVTYS) (DDBMS - Distributed Database Management System), geleneksel merkezi veri tabanı

sistemlerine göre potansiyel avantajlara sahip olduğu belirtilmekle birlikte, dezavantajların da olduğu belirtilmiştir. Klasik DVTYS siteler arasındaki ağda ek hata noktaları oluşturabilmektedir. Veri çoğaltma işlemlerinin sağlanması süreçlerinin ise dağıtılmış DVTYS'ye ekstra bir karmaşıklık eklemektedir. Ayrıca, verilerin bütünlük kontrolü ve güvenliği daha zor olmaktadır. Bu sebeple veri tabanı tasarımı daha karmaşık hale gelmektedir. Elektronik oylama sistemlerinde klasik veri tabanlarının kullanımı yerine blok zincirinin kullanılması ile veri tabanının yedekliliğinin ve veri bütünlüğünün sağlanmasında yardımcı olabileceği belirtilmektedir. Ayrıca, bazı araştırmacılar veri bütünlüğünü sağlayabilmek için kimlik kartlarının sisteme uyumunu da sağlamışlardır. Bu sayede yetkisiz girişleri engelleyerek, kimlik doğrulmasını kimlik kartı ile yapmışlardır. (Kimlik numarası (Bulut vd. 2019), Dijital kimlik kartı (Venkatapur vd. 2018)). Khoury ve arkadaşları ise cep telefonu ve şifre eşleştirmesini kayıt sırasında kullanılmasını önermişlerdir (Khoury vd. 2018). Bunlardan farklı olarak Adiputra ve arkadaşları ile Akbari ve arkadaşları tarafından seçmenin parmak izi, iris ve yüz özellikleri gibi biyometrik özelliklerinin kimlik doğrulama için kullanılması önerilmiştir (Akbari vd. 2017, Adiputra vd. 2018,). Kimlik ve biyometrik entegrasyonun yapıldığı sistemlerde doğrulama için devletlerin vatandaşlarına sağladığı kimlik numarası ve biyometrik bilgilerini kullanmışlardır. Böylece hileli oy kullanma, kimliği belirsiz olan kişilerin oy kullanması ve aynı kişinin sahte kimliğe sahip olması gibi sorunların ortadan kalkacağı vurgulanmıştır. Venkatapur ve arkadaşları Aadhar adı verilen kimlik kartının entegre edildiği blok zinciri tabanlı oylama sistemini önermiştir. Bu yaklaşımla şeffaflığı sağladığı, daha doğru, şeffaf ve adil bir seçim sistemi sağlanabileceği vurgulanmıştır (Venkatapur vd. 2018). 2019 yılında yapılan Gao ve arkadaşlarının olası kuantum bilgisayar saldırılarını engellemek için kod tabanlı ortak anahtar şifreleme algoritması uyarlamışlardır. Sonuç olarak, bu önerinin şeffaflık sağladığı, ancak küçük çaplı seçimler için daha uygun olduğu sonucuna varmışlardır (Gao vd. 2019)

e) Uzlaşma (Consensus): Fikir birliği algoritması dağıtık sistemlerde veriler üzerinde anlaşmayı ve işlemlerin doğru işlenmesini sağlayan mekanizma olarak kullanılmaktadır. Luo ve arkadaşları blok zincirinde seçimlerin güvenliğini ve verimliliğini artırmak için DPoS uzlaşma algoritmasını önermişlerdir. Tüm sürecin merkeziyetçiliğini ve adaletini sağlayan seçim algoritması oluşturulduğu belirtilmiştir (Luo vd. 2018). 2017'de McCorry ve arkadaşları blok zincirine dayalı internet oylama protokolü önermişlerdir. Ancak bu sistem küçük çaplı seçimleri desteklemek için planlanmıştır. Seçmenler, oylarını gizlemek ve oyların geçerliliğini kanıtlamak için Sıfır Bilgi Kanıtı kullanarak akıllı sözleşmeye şifreli oylar göndermişlerdir. Sistemlerinde "açık oy ağı (open vote network)" olarak adlandırılan merkezi olmayan iki aşamalı bir protokol kullanılmıştır. Ancak, küçük ölçekli bir toplantı odası oylamasını desteklemek için tasarlanmıştır (McCorry vd. 2017). 2018'de Hjálmarsson ve arkadaşları özel Ethereum altyapısını kullanan bölgesel seçimlere yönelik olarak tasarladıkları seçim sisteminde seçim sonuçlarını akıllı kontratlarda saklamışlardır. Bu sisteminde küçük ölçekli uygulamalar için uygun olduğu belirtilmiştir (Hjálmarsson vd. 2018).

Li ve arkadaşlarının oy ispatı (Proof of Vote (POV)) fikir birliğini uyguladıkları yöntemi iş kanıtı (POW) ile karşılaştırdıklarında, kullandıkları yöntemin kontrol edilebilir güvenlik ve işlem doğruluğu sağlamak için düşük bir gecikme süresine sahip olduğu belirtilmiştir (J. Li vd. 2017). Ayrıca, Leonardos ve arkadaşları bir çarpımsal ağırlık algoritması (multiplicative weight algorithm) ekleyerek PoS uzlaşma mekanizmasını geliştirerek uygulamışlardır. Uygulamalarında hesaplama yükü, geçersiz blok ve güncelleme şeması gibi bilgilerin manipülasyonu ile bağlantılı yeni riskler ortaya çıkardığı belirtilmiştir (Leonardos vd. 2019).

İncelenen makalelerde genellikle blok zincirinin seçim sistemlerinde kullanılabileceği vurgulanırken, özellikle seçimlerin mahremiyetini korumanın ve güvenliğin önemine yönelik vurgulamaların çalışmaların ortak noktasını oluşturduğu görülmüştür.

3.3 Blok Zinciri Sisteminin Katkıları

Son yıllarda blok zinciri tabanlı elektronik oylama sistemleri önerilmeye başlanmıştır (Osgood 2016). Bir blok zinciri destekli e-oylama sistemi seçim süreci seçim öncesinde ve sırasında çok kritik görevler gerektirmektedir. Bunlar seçim hazırlık hizmetleri, tüm oylama sistemlerinde olduğu gibi seçim öncesinde mevcut seçmen listesi, adaylar, sandık tasarımı hazırlanmalıdır. Seçmen kaydından sonraki aşamada diğer sistemler den farklı olarak, seçmenler oylama işlemleri yapmak için bir oylama tokenı kullanmaları gerekmektedir. Gerçek bir oylama sisteminin tasarımında, daha güvenli bir ortam oluşturmak için özel blok zinciri yapısının kullanılması ve bağımsız kontrol düğümünün dâhil edilmesi gerekmektedir. Bu düğümler birbirleriyle bağlantılıdır ve senkron bir özellikte çalıştığı için hem yedeklilik hem de izlenebilirlik imkânı vermektedir.

Blok zinciri çerçevesinde fikir birliği mekanizmaları ve işlemleri tarafsız üçüncü taraf kuruluşların izlemesine ve dağıtılmış ağına göre tasarlanan düğümlerden oluşturulmalıdır. Bu düğümlerin amacı, işlemleri mutabakat algoritmasına göre çıkarmak ve oylama defterine bloklar eklemek şeklinde olmalıdır. Veriler kriptografik olarak saklanmalı ve bağımsız düğümlerinde katılımıyla seçim sonuçları denetlenerek açıklanmalıdır.

Araştırma sonuçlarından, blok zinciri sistemlerinin elektronik oylama sistemlerine sağlayacağı katkılar aşağıdaki gibi sıralanabilir;

a) DDOS saldırıları; günümüzde uzmanların siber saldırılarda karşılaştığı en kritik zorluklardan biri olduğu belirtilmektedir. DDoS saldırısının bir sonucu olarak blok zinciri ağlarındaki bazı düğümler çevrimdışı olursa, sistem dağıtılmış yapısı nedeniyle herhangi bir kesinti olmadan çalışmaya devam edebileceği belirtilmektedir. Düğümler tekrar çalıştığında tutarlılık sağlamak için her şey tekrar senkronize edilerek çalışabilmektedir. Bu sayede veri kaybı riski de oluşmamaktadır. Blok zincirinin genel mimarisi tek hata noktalarından kaçınmak için tasarlanmaktadır. Blok zinciri düğümleri bağımsız ve aynı anda

çalışmaktadır. Bu nedenle, blok zinciri özellikle elektronik oylama sistemleri içinde yüksek kullanılabilirlilik sağlayacağı belirtilmektedir (Akbari vd. 2017, Hjálmarsson vd. 2018, Pathak vd. 2018).

b) Blok zinciri yapıları işlemleri kaydetmek için değişmez bir defter oluşturdukları kabul edilmektedir. Tüm katılımcılar dağıtılmış defterlerdeki kayıtlarına erişebilmektedir. Sistem katılımcılarının hiçbiri kaydedilen işlemleri değiştiremez veya silinemez olduğu belirtilmektedir. Bu da verilerin bütünlüğü ve güveni açısından sağlamlık ortamı tesis etmektedir (Hanifatunnisa ve Rahardjo 2017).

c) Blok zinciri tabanlı e-oylama hem şeffaflık hem de gizlilik sağladığı belirtilmektedir. Katılımcılar veya bağımsız gözlemciler, blok zincirinde depolanan oylama sonuçlarını takip edip onaylayabilmektedir. Böylelikle seçim izlenebilirliğini sağlayabilmekte ve güvenilirlik seviyesini artırılabilmektedir (Hjálmarsson vd. 2018).

d) Blok zinciri sistemleri, uzun vadede daha ucuz bir maliyet vaat etmektedir. Dağıtık mimaride güvenli bir veri depolama sistemi kurmak ve işletmek, yüksek maliyet ve güvenlik riskleri içermektedir. Blok zincirinin standart veri tabanı uygulamalarından daha güvenli ve daha ucuz olduğu belirtilmektedir.

e) Bazı e-oylama yöntemlerinde oyların çeşitli oylama alanlarında gözden geçirilmesi ve ardından merkezi birimlerde toplanması gerekmektedir. Bu süreçler oldukça fazla zaman alırken seçim sonuçlarının açıklanması da uzun sürebilmektedir. Blok zinciri ile seçim sonuçları saatler yerine dakikalar içinde güvenli bir şekilde açıklanabileceği belirtilmiştir (Kshetri ve Voas 2018).

f) Artırılmış güven ortamı sayesinde seçimlere katılım oranlarının artırabileceği belirtilmektedir (Kshetri ve Voas 2018). Gelişim perspektifinden bakıldığında, e-oylama sistemlerinin temel avantajlarından biri, hem geliştirme hem de operasyonlar için gömülü olabilecek çeşitli kontroller sağlamasıdır. Örnek vermek gerekirse, seçmen anonimliği, blok zinciri

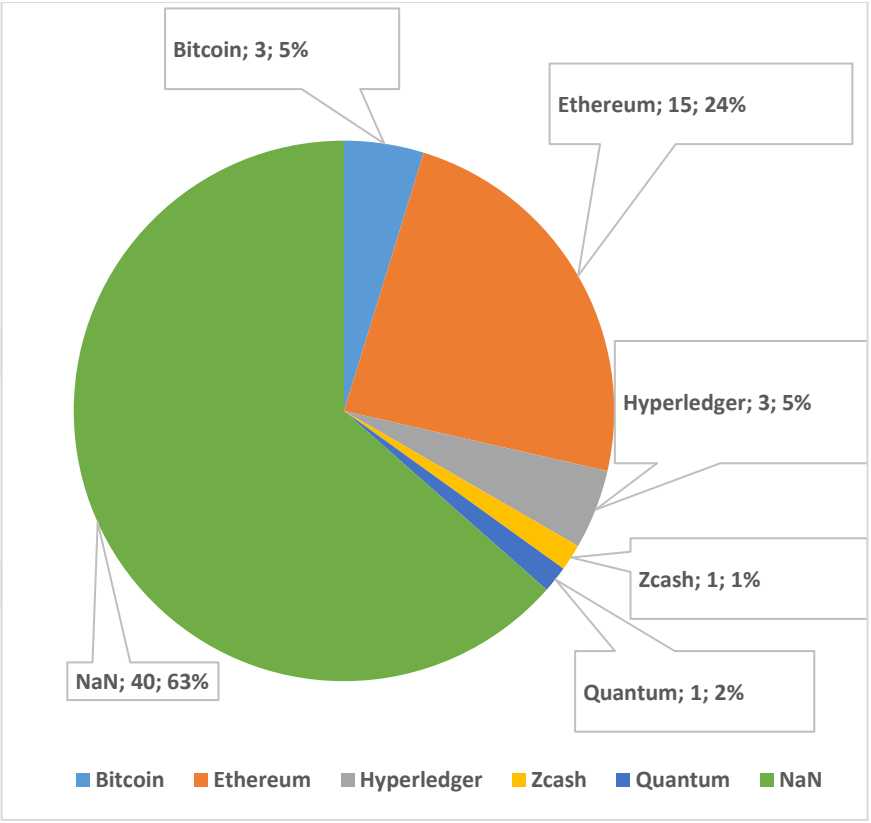
kullanılırken kurcalamaya dayanıklı yapılardan yararlanılarak kriptografik teknikler kullanılarak gerçekleştirilebilmektedir. Bu kontrol noktalarının, vatandaşların sisteme olan güvenini artırmada olumlu bir etkisi olabileceği değerlendirilmektedir. Vatandaşlara; seçmen kimliğinin nasıl doğrulanacağı, çoklu oy kullanımının nasıl engellendiği, vatandaşların oylarının nasıl gizli kaldığı ve doğru sayıldığı bildirilmelidir. Ek olarak, geliştirme sürecinde bağımsız doğrulama ve onaylama sistemlerinin kullanımının ekstra güvence sağlayabileceği değerlendirilmektedir.

3.4 En Çok Tercih Edilen Blok Zinciri Altyapısı

Blok zinciri altyapısı, blok zinciri uygulamalarının geliştirilmesine izin veren platformlar olarak yer almaktadır. Bitcoin, Ethereum, Hyperledger ve R3 Corda, en ünlü blok zinciri platformu olarak öne çıkmaktadır. Seçilen makalelerin detayları analiz edilerek en çok hangi sistemlerin tercih edildiği tespit edilmek istenilmiştir. Çalışmaların çoğunda, blok zinciri tabanlı e-oylamanın genel fikri, uygulanabilir olduğu ve buna bağlı genel konuları ele aldıkları görülmüştür. Birçok makalede teknik detayların ve uygulama önerilerinin açıkça belirtilmediği tespit edilmiştir. İncelenen makalelerde bilgisi verilen sistemlerin veya test platformu geliştirilen blok zinciri platformu kullanımı dağılımı Şekil 3.5 'de gösterilmiştir. En çok tercih edilen blok zinciri platformunun % 24 ile akıllı sözleşme özelliğini de içeren Ethereum platformunun olduğu tespit edilmiştir. Ethereum ‘un açık kaynaklı bir blok zinciri platformu olmasının, çok çeşitli geliştiricilerin merkezi olmayan uygulamalar oluşturmasına ve dağıtmasına izin vermesinin birçok araştırmacı tarafından tercih edilen platform olmasını sağladığı belirtilmiştir.

Blok zinciri teknolojisinin artan popülaritesi geniş kullanım alanlarına erişmesi neticesinde ölçeklenebilirlik sorunu da araştırmaları ilgisini çekmeye başlamıştır. Mevcut durumda zorluk derecesinin değiştirilmesi veya blok büyüklüklerinin ihtiyaca göre değiştirilebilmesi işlem sürelerini kısaltabilcektir. Ayrıca, bu problemin çözümünde yardımcı olabilceğini belirten bazı alternatif zincir altyapılarıda önerilmeye başlanmıştır. Holochain blok zinciri alt yapısında işlem ücreti ve blok onayı bekleme süresinin olmadığı belirtilerek

ölçeklenebilirlilik konusunda yardımcı olduğu belirtilmektedir (Holochain 2022). Hyperledger'de bu doğrultuda bazı iyileştirmeler yapmış ve saniyede 20000 işlem yapabildiklerini belirtmişlerdir (Nasir vd. 2018).



Şekil 3.5 Blok zinciri platformu kullanım oranı diyagramı

3.5 Geçerlilik Değerlendirmesi

Sistematik bir haritalama çalışması yürütürken ortaya çıkabilecek çeşitli eksiklikler olabilmektedir. Örneğin, tüm ilgili çalışmalar veya bilgi kaynakları tanımlanmayabilmektedir (Vegendla vd. 2018). Bu eksiklikleri ortadan kaldırmak için farklı arama kriterleri belirlenmiştir. Ayrıca konuyla ilgili çeşitli veri tabanlarından taramalar gerçekleştirilmiştir. Farklı kriterler ve mantıksal operatörler uygulayarak kapsamın genişletilmesi hedeflenmiştir. Çeşitli anahtar kelime kombinasyonlarını kullanarak ilgili tüm makalelerin tespit edilmesi amaçlanmıştır.

Konu tamamen yeni olmasına rağmen, hariç tutma kriterlerinden sonra elde edilen araştırmaların çoğunun 2018 – 2019 yıllarında yayınlanmış olduğu tespit edilmiştir. Bu nedenle, konuyla ilgili eksik makale incelemesinin çalışmamızın bulgularını etkilemeyecek kadar az olduğu değerlendirilmiştir. Tarama yapılmayan diğer veri tabanlarında yer alan makalelerin ise, seçilen veri tabanlarının iyi bilenen bilimsel veri tabanları olması sebebiyle hariç tutulanlarında benzer özellikler taşıyacağından sonuçları etkilemediği değerlendirilmiştir.

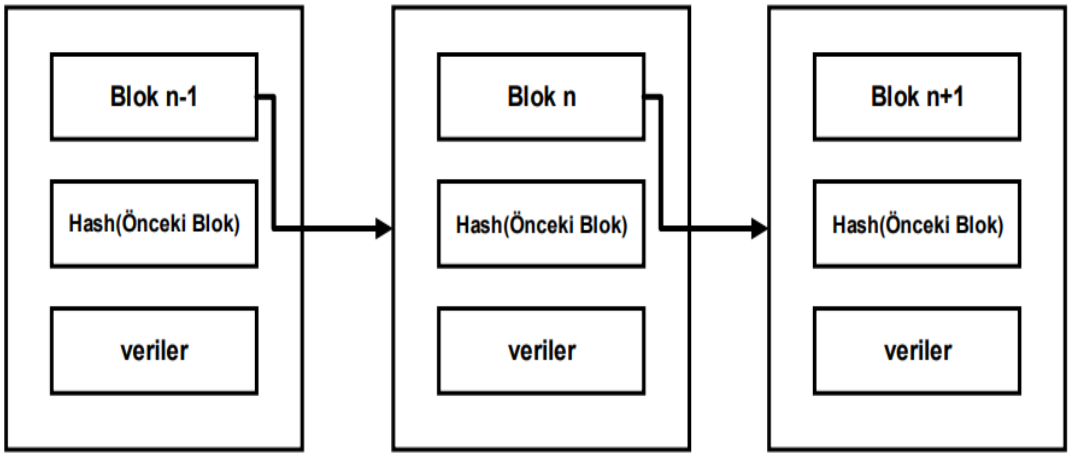
Silva ve arkadaşları dış geçerlilik için, çalışma sonuçlarının diğer durumlar, insanlar ve zamanlar için genellenebileceği anlamına geldiğini belirtmişlerdir (Silva vd. 2017). Sistematik incelememizde, araştırma sonucunda elde edilen verilerin mevcut blok zinciri araştırmaları ve eğilimleri açısından genel sonuçları yansıttığı düşünülmektedir. Çünkü makaleler en son 2010 – 2019 yılı sonuçlarını ve otuz farklı ülke araştırmacılarının bakış açılarıyla yayınladıkları makalelerinin değerlendirilmesi neticesinde elde edilmiştir.

4. BLOK ZİNCİRİ TEKNOLOJİSİ

Bu bölümde, e-oylama sistemi tasarımı bağlamında faydalı olabilecek blok zinciri teknolojilerine genel bir bakış sunulmaktadır. Blok zinciri konsepti, ilk olarak 1991 yılında dijital belgelerdeki değişiklikleri önlemek amacıyla zaman damgası olarak tasarlanmıştır (Haber ve Stornetta 1991). 2008 yılında Satoshi Nakamoto (Nakamoto 2008), blok zinciri teknolojisini kullanarak tamamen dağıtılmış bir dijital para birimi sistemi geliştirmiştir. Birkaç yıl boyunca, bu sistem toplum tarafından fark edilmemiştir. Ancak Bitcoin 'in (Anonymous 2020a) 2017 – 2018 yılları arasında aşırı değerlenmesinden sonra (Anonymous 2020b), ilgi çekmeye başlamıştır. Son zamanlarda kripto para birimleri ve bunların altında yatan teknoloji olan blok zinciri araştırmacılarında ilgi odağı olmaya başlamıştır. Günümüzde, çok sayıda insan blok zinciri teknolojisini internet kadar yenilikçi olabileceğini düşünmektedir (Sadouskaya 2017).

Bir blok zinciri, eşler arası merkezi olmayan bir şekilde çalışan, geçerli işlemlerden oluşan bir blok kümesi olarak tanımlanmaktadır. Blok zinciri sisteminde, herhangi bir düğüm, ağ içindeki tüm düğümlere yayılabilen bir işlem başlatabilmektedir. Başlatılan işlem doğrulandıktan sonra, blok zincirine eklenerek işlemler kayıt altına alınmaktadır (Mohanta vd. 2019). Blok zinciri ağında gerçekleşen tüm işlemleri kaydeden dağıtılmış bir veri tabanı olarak ta değerlendirilebilmektedir. Bu veriler ağın diğer katılımcıları arasında paylaşılarak kopyalanmaktadır (Şekil 4.1). Blok zincirinin temel özelliği, katılımcıların güvenilir bir üçüncü tarafa ihtiyaç duymadan birbirleri arasında güvenli bir şekilde iletişim kurmasına ve veri göndermesine izin vermesidir. Blok zinciri, her bloğun kriptografik karması ile tanımlanmış sıralı bir blok listesidir. Her blok, kendisinden önce gelen bloğu referans almaktadır. Bu şekilde oluşturulan veri zincirlerin den oluşmaktadır. Bir blok oluşturulduktan ve blok zincirine eklendikten sonra, bu bloktaki işlemler değiştirilemez ve geri alınamaz duruma gelmektedir. Bu da, işlemlerin bütünlüğünü ve doğruluğunu sağlamak için kullanılmaktadır (Alharby ve van Moorsel 2017). Ağda başlatılan işlemler, madenciler tarafından doğrulanmaktadır. Madenciler, bir işlemi doğrulamak,

göndericiyi ve işlemin içeriğini kontrol etmeye yardım etmektedir. Veri madencileri, blok zincirini oluşturan blokları üretmek için her işlemde sunulan verileri doğrulamak için sürekli olarak kaynaklarını paylaştıklarından blok zinciri ağının hayati bir parçası olarak çalışmaktadır. Madenciler yaptıkları başarılı işlemler neticesinde kullanılan blok zinciri türüne eşdeğer bir para birimine ile ödüllendirilmektedir.



Şekil 4.1 Blok zinciri yapısı

Her işlemin blok zincirine tanıtılmadan önce doğrulanması gerekmektedir. Böylece kötü niyetli kullanıcıların sistemi kötüye kullanması ve bozması engellenmektedir. Genel olarak madenciler matematiksel bir bulmacayı çözdükten sonra işlem bloğunu oluşturup ardından bu bloğu ağa iletmektedir. Ağdaki diğer düğümler, üretilen bloğun doğruluğunu kolayca onaylayarak sisteme dâhil edilmesine izin vermektedir (Pilkington 2015).

Blok zinciri sistemleri de zaman içinde gelişim göstermeye başlamıştır. Bunlar 3 kategoride ele alınabilmektedir (Bashir ve Safari 2017).

a) Blockchain 1.0; Bitcoin ‘in icadıyla tanıtılmıştır. Temelde kripto para birimleri için kullanılmaktadır. Ayrıca, daha sonra ortaya çıkan diğer alternatif madeni paralar da bu kategoriye girmektedir. Sistem ödeme programları gibi temel uygulamaları içermektedir.

b) Blockchain 2.0; finansal hizmetler tarafından kullanılmaktadır. Bu nesilde sözleşmeler sunulmuştur. Çeşitli finansal varlıkları, takasları ve tahvilleri gibi uygulamaların geliştirilmesine katkı sağlamıştır.

c) Blockchain 3.0; finansal hizmetler endüstrisinin ötesindeki uygulamaları geliştirmek için kullanılmaktadır. Sağlık, medya, sanat ve adalet gibi daha genel amaçlı alanlarda kullanılabilmektedir (Cheng vd. 2018) .

4.1 Blok Zinciri Kullanım Alanları

Blok zinciri tabanlı yaklaşım, geleneksel istemci sunucu mimarisi yaklaşımında kullanılan diğer sistemlerden bazı farklılıklar göstermektedir. Blok zinciri aslında doğrudan sistemdeki tüketiciler ve sağlayıcılar arasında gerçekleştirilen tüm işlemlerin dağıtılmış bir defter üzerinden takibi olarak görülmektedir. Genel çalışma prensibi olarak blok zinciri, somut bir üçüncü tarafa ihtiyaç duymadan karşılıklı güven oluşturulmasına izin vermektedir. Blok zinciri, kripto para birimleri bağlamında yaygın olarak bilinmesine rağmen, potansiyeli dijital paranın çok ötesine farklı kullanım alanlarında da uygulamaların geliştirilmesiyle ortaya çıkmıştır (Abdelwahab 2017). Bir çeşit dağıtık kütük teknolojisi olan blok zinciri, dünya çapında dağıtılan açık ve güvenli bir veri tabanına benzer şekilde de görülebilmektedir. Bu nedenle, bu altyapı sadece kripto para birimi ve finans sektörlerinde değil, birçok farklı alanda da kullanılabileceği görülmüştür. Başta tarım (Shakhbulatov vd. 2019), sağlık hizmeti (Shahnaz vd. 2018), akıllı şehir (Xie vd. 2019), gayrimenkul (Latifi vd. 2019), eğitim (Turkanović vd. 2018), eğlence (Bilow 2020), fikri mülkiyet (Ajay vd. 2018) olmak üzere birçok alanda kullanım fırsatları araştırılmaya başlanmıştır. Son zamanlarda firmaların farklı alanlarda blok zinciri uygulamalarını işletmelerine entegre etmeye başladıkları görülmektedir. Bu sayede işletmeler süreçlerin yönetimini daha şeffaf hale getirmeyi amaçlamaktadır. Özellikle kimlik ve sahtekârlık ile ilgili konular olmak üzere çeşitli güvenlik endişelerini gidermeye yardımcı olduğu düşünülmektedir.

Blok zincirinin uygulanabilir bir diğer alanı ise lojistik yönetimi ve B2B ticaretinin sürdürülebilir operasyonları olarak görülmektedir. Tüketiciler ve üreticiler arasındaki işbirliğini teşvik ederek, şirketlerin kaynaklarını ve yeniden kullanım süreçlerini iyileştirmelerine yardımcı olarak yükselen bir alan oluşturmaktadır. Blok zinciri bu süreçlerin ihtiyaç duyduğu güvenlik, şeffaflık ve izlenebilirlik özelliklerin sunmaktadır. Tedarik zinciri yönetimi üzerinde uçtan – uca tedarik zincirindeki tüm süreçlerin izlenebilmesini sağlamaktadır. Bu tür kullanımlarda teslimat aşaması tamamlandıktan sonra ödemeler otomatik olarak yapılabilmektedir. İşlemler taraflarca izlendiğinden ürünlerin uçtan uca takibinde büyük ölçüde süreç iyileştirmelerine yardımcı olması beklenmektedir. Böylelikle tüketiciye ürünü satın almadan önceki süreçlerdeki durumları hakkında da detaylı ve doğru bilgi verilebilmesi hedeflenmiştir (Tan vd. 2020).

Blok zincirinin finans ve tedarik zinciri yönetimindeki potansiyel faydaların yanı sıra hizmet sektöründe ve internet tabanlı uygulamalarda da kullanılabilmektedir. Bu alanlardan biri olan enerji sektörü blok zincirinin kullanım alanları arasında araştırmalara konu olmaktadır. Yerel enerji ticareti ve elektrikli araçların şarj işletmeleri alanlarında da projeler önerilmiştir (Yahaya vd. 2020). Araçların önceden tanımlanmış IoT (Internet of Thing) cihazları üzerinden haberleşme yapması veya enerji alıp satması mümkün olabilmektedir (Gupta vd. 2018). Gerçek zamanlı olarak IoT cihazları üzerinden toplanan verilerin blok zincirine kaydedilerek, büyük veri analizinde kullanılması da farklı bir araştırma konusu olmuştur (Javed vd. 2020, Villegas-Ch vd. 2020)

Sigorta endüstrisi, blok zinciri kullanan yeni bir örnektir. Günümüzde sigorta sektörü karşılıklı güven ilişkisine dayanarak çalışmaktadır. Ara sıra oluşan hata veya gecikmelerin gelecekte, karşılıklı güven ortamının tesis edilmesiyle hızlı bir şekilde çözümler sunabileceği değerlendirilmiştir (Raikwar vd. 2018). Sağlık sektörü de blok zinciri teknolojisini kullanan sektörler arasındaki yerini almaya başlamıştır. Bu sektörde sağlık hizmeti sağlayıcıları, klinik araştırmalar, eczacılar ve hastalar gibi kilit paydaşların elektronik tıbbi kayıtlara güvenli, daha hızlı ve güvenilir erişim

sağlamasında yararlı bir araç görevi görebileceği belirtilmiştir (Hölbl vd. 2018, Raikwar vd. 2018).

Yakın gelecekte bulut depolama (Li vd. 2017), ulaşım sistemleri (Yuan ve Wang, 2016), siber güvenlik (Yazdinejad vd. 2020), kimlik yönetimi (DeCusatis vd. 2018), emlak ve tarım izlenebilirliği (Demestichas vd. 2020, Osmanoglu vd. 2020) alanlarında blok zinciri entegrasyonu yapılmış çözümlerden faydalanılacağı araştırmacıların ilgilendiği başlıklar arasında yer almaktadır. E-oylama sistemlerinde kullanılabilirliği de umut verici bir alan olmakla birlikte öne çıkmaktadır (Zhao ve Chan 2016).

4.2 Blok Zinciri Ağ Türleri

Blok zinciri çalışma prensibi olarak üç türe ayrılmaktadır, farklı güvenlik ve işlevsellik ihtiyaçlarına göre genel, özel ve konsorsiyum blok zincirleri olarak tanımlanabilmektedir. Farklı uygulamalar, ihtiyaca göre farklı mimari türlerine göre tasarlanması gerekebilmektedir. Çizelge 4.1'de, sistem tasarımında dikkate alınacak yönetim, katılımcı türü, merkezileştirme, fikir birliği ve işlem süresine özelliklerine göre sınıflandırması verilmiştir. Herkese açık blok zincirinde doğrulama, blok zincirindeki tüm düğümlere dağıtıldığı için merkezi bir otorite bulunmamaktadır. Bu tür blok zincirindeki ağ yapısında, tüm bilgilerin ağdaki herkesin okuyabileceği ve fikir birliğine katkıda bulunabilecek tüm eşlere açık olarak tasarlanması gerekmektedir. Özel blok zinciri ise, yalnızca belirli sayıda katılımcı tarafından kullanılmaktadır. İzne dayalı olarak da bilinen özel blok zincirinde, yalnızca belirli haklara sahip belirlenmiş düğümler, bilgilerin işlenmesine ve fikir birliği mekanizmasına katkıda bulunabilmektedir. Özel blok zincirinde ağdaki yazma izinlerinin tek bir grupta merkezileştirilmiş olarak yapılandırıldığından herkese açık olarak çalışmamaktadır. Özel blok zincirindeki kısıtlı sayıda kullanıcı erişimi ile gerçekleştirildiğinden bu tür yapıda işlem doğrulaması için daha az hesaplama gücüne ihtiyaç duyulmaktadır (Dinh vd. 2017). Bu sayede halka açık blok zincirinin aksine düşük miktarda sınırlı kaynakla kontrollü erişim sağlandığı için ağ içinde daha

az güvenlik olacağı anlamına gelebilmektedir. Öte yandan, işlemlerin doğrulanmasının daha az zaman alması, sistemin daha verimli kullanılmasını sağlayan hızlı işlem doğrulaması ile sonuçlanması beklenmektedir (Lin ve Liao 2017). Son olarak, konsorsiyum blok zinciri ise önceden belirlenmiş belirli düğümlerin ve farklı bireylerin de dâhil edildiği bir yapı ile oluşturularak çalışması sağlanmaktadır. Bu nedenle, mutabakat prosedürünün önceden seçilmiş düğümler tarafından kontrol edildiği halka açık blok zincirine göre daha fazla güvenlik özelliği içerdiği belirtilmektedir (Hanifatunnisa ve Rahardjo 2017).

Çizelge 4.1 Blok zinciri çeşitleri

Özellik	**Açık**	**Özel**	**Konsorsiyum**
Yönetim	Merkezi Yönetim Yok	Tek Organizasyon	Çoklu Organizasyon
Katılım	İzinsiz	İzne Bağlı	İzne Bağlı
Merkeziyetçilik	Yok	Var	Kısmi
Verimlilik	Düşük	Yüksek	Yüksek
Uzlaşma Tayini	Tüm Madenciler	Organizasyona Katılanlar	Seçilmiş Madenciler
İşlem Süresi	Uzun	Kısa	Kısa

Özel blok zincirlerinin popülaritesinin artmasına rağmen, halka açık blok zincirleri en çok kullanılan blok zinciri türü olarak ön planda kalmaya devam etmektedir. Açık ağda fikir birliğinin oluşturulması, daha fazla düğüm olduğu için daha uzun sürmektedir. Bu nedenle halka açık bir blok zinciri, işlemleri yürütmek için daha fazla elektrik tüketimi yapmaktadır. Konsorsiyum yapısındaki sistemler özel veya halka açık blok zinciri arasında bir yerde konumlanmaktadır. Konsorsiyum blok zincirinde, fikir birliği yalnızca önceden seçilmiş bir dizi düğüme bağlı olarak çalışmaktadır. Bu tür zincirde yer alan düğümler sistemdeki bilgilerin saklanmasına ve işlemlerin başlatılmasına yardımcı olmak için kullanılabilmektedir (Zhang vd. 2018, Tang vd.

2019). Ağ içindeki verileri okumak için okuma hakları halka açık tasarlanabilmektedir veya katılımcılarla sınırlı izinler verilebilmektedir. Bu nedenle söz konusu blok zincirinin cüzdanına sahip olmayan kişilerin işlemleri görüntülemesine izin verilmemektedir. Özel blok zinciri ile hibrid blok zinciri arasındaki ayrım; özel blok zincirinin bir dereceye kadar kendisine bağlı kriptografik denetlenebilirlilik derecesine sahip merkezi bir sistem olması, buna karşılık konsorsiyum blok zincirinin halka açık bir blok zincirine daha çok benzemesi ve bu nedenle merkeziyetçilik açısından daha merkezi olmamasıdır. Özel blok zincirleri, halka açık blok zincirleri kadar popüler olmasa da birkaç avantajı bulunmaktadır. Halka kapalı blok zincirine sahip olma fikri, blok zincirinin fikir birliği mekanizmasını etkileyen herhangi bir dış erişimin olmadığı anlamına gelmektedir. Ayrıca, ağ üzerinden işlemlerin yürütülmesi için gereken daha düşük donanım gereksinimleri nedeniyle işlem maliyeti büyük ölçüde azalmaktadır. Ayrıca işlem hızı her zaman halka açık blok zincirinden daha yüksek olmaktadır. Bu nedenle, özel blok zincirlerinin küçük ve orta ölçekli ağlarda daha uygun olduğu belirtilmektedir (Sabry vd. 2019).

4.3 Blok Zinciri Çalışma Prensibi

Bitcoin protokolünün icadından sonra, blok zinciri her türlü elektronik işlem verilerini depolamak için çok güvenli, dağıtık bir veri tabanı altyapısı sağlayan dünyadaki en güçlü bilgi işlem ağı haline gelmiştir (Noizat 2015). Bir çeşit dağıtık kütük teknolojisi olan blok zinciri son yıllarda alternatif sistemlerinde katılımıyla daha da gelişmektedir. Blok zinciri tasarımı, kriptografik olarak bağlı olan sürekli büyüyen kayıt listesi nedeniyle kurcalamaya karşı dayanıklı veriler sunmayı vaat etmektedir.

Sistem merkezi bir kayıt defterindeki, sistemin düğümleri arasında dağıtılmış verilere dayanmaktadır. Bir blok zinciri düğümü, bloğa girişlerdeki verileri ekleyerek ilerler ve deftere eklenen veriler daha sonra güncellenemez veya silinemez olarak ifade edilmektedir. İşlemler düğümler arasında dağıtılarak çoğaltılmaktadır. Ayrıca, sıralı

olarak oluşturulan bloklar şifrelenir, bir özet fonksiyonu kullanılarak imzalanır ve bloğa zincirler halinde eklenerek oluşturulmaktadır. Blok zinciri teknolojisinde kullanılan bir diğer önemli kavram ise fikir birliği kavramıdır. Blok zinciri üzerindeki fikir birliği algoritması, tüm işlemlerin geçerli ve orijinal olmasını sağlamak için kullanılmaktadır. Her düğüm bir işlemi doğruladıktan ve işlemin yürütülebileceği sonucuna vardıktan sonra, tüm düğümler arasında fikir birliği içinde olduğu bildirilmektedir. Şayet, bir kullanıcı geçersiz veya bozuk bir işlem göndermeye çalışırsa da, düğümler bir fikir birliğine varmaz ve işlem blok zincirine dâhil edilmemektedir. Böyle bir sistemde, hem kullanıcılar hem de bilgisayar işlemleri blok zinciri ağında olduğu için yedekleme hizmetleri oluşturmaya da gerek kalmamaktadır. İş kanıtı (Proof of Work-PoW) veya Teminat kanıtı (Proof of State-PoS) modelleri, blok zinciri altyapılarında fikir birliği mekanizmaları olarak sıklıkla tercih edilmektedir (Pawlak ve Poniszewska-Marańda 2021).

Blok zinciri teknolojisinin gelecekteki internet sistemlerinin inşası için büyük bir potansiyele sahip olmasına rağmen, bir takım teknik zorluklarla karşı karşıya olduğu da birçok araştırma neticesinde ortaya konulmaktadır. Birincisi, ölçeklenebilirlik büyük bir sorun olarak gösterilmektedir. Bitcoin blok boyutu şu anda 1 MB ile sınırlıdır ve yaklaşık olarak 10 dakikada bir blok oluşturulmaktadır. Bitcoin ağı, yüksek frekanslı işlemler (kredi kartı işlemleri gibi) söz konusu olduğunda yetersiz kalabilmektedir (Zheng vd. 2018). Blok büyüklüğünde değişiklikler yapılarak işlem süreleri değiştirebilmektedir.

Blok zinciri altyapısı farklı katmanlardan oluşmaktadır. Katman yapısı veri, ağ, fikir birliği, teşvik, akıllı sözleşme ve uygulama katmanından oluşmaktadır (Mohanta vd. 2019, Wang vd. 2019, Ferdous vd. 2020, Ismail ve Materwala, 2020, Yan vd. 2020) (Çizelge 4.2). Veri katmanının işlevi, verileri blokta depolamaktır. Değişken boyutlu verilerin sabit uzunlukta bir çıktısını üretmek için bir karma işlevi uygulanmaktadır. Geri dönüşü olmayan tek yönlü bir fonksiyon olduğundan işlenen veriler hesaplanan özet değerinden geri alınamamaktadır. Böylece, blok zincirinin bütünlüğü sağlanmış olmaktadır.

Blok zincirinin ağ katmanı, eşler arası (P2P) bir ağ yapısı üzerinde çalışmaktadır. Eşler arası uygulamalar genellikle güvenilir bir yetkiye sahip olmayan eşler arasında görevleri bölen dağıtılmış mimariler tarafından yönetilmektedir. İki veya daha fazla makine arasında iletişim kurmak, işlemek ve blok zincirini çoğaltmak için bir ağ programı protokolü olarak kullanılmaktadır (He vd. 2018). Ağdaki her düğüm kaynaklarından sorumludur ve hem sunucu hem de istemci olarak hizmet verebilmektedir.

Çizelge 4.2 Blok zinciri katmanları

Katmanlar	**Özellikler**
Altyapı Katmanı	Akıllı Sözleşmeler, Script Kodlar, Düğümler
Uzlaşma/Platform Katmanı	Replikasyonlar, İşlemler, Özet Fonksiyonları, Uzlaşma Modelleri
Ağ Katmanı	P2P ağ, Transmisyon ve doğrulama mekanizması
Veri Katmanı	Blok yapısı, zincir yapısı,

Uzlaşma katmanı, blokların sırasını yöneten dağıtılmış konsensüs mekanizmasını yönetmektedir. Teşvik katmanının amacı ise düğümlerin blok zincirinin güvenlik doğrulamasına katılması için sağlamaktadır. Sözleşme katmanı, akıllı sözleşme yardımı ile kurallara göre işlemler başlatmaktadır (Wang vd. 2019, Ferdous vd. 2020).

4.3.1 Blok zinciri temel kavramları

Bu bölümde blok zincirlerinin tam olarak anlaşılması için sıklıkla karşılaşılan kavramlar kısaca tanımlanmıştır.

Düğümler (Nodes): Bir blok zincirindeki düğüm, dağıtılmış bir defter ağına katılan cihaz olarak ifade edilmektedir. Bu bilgisayar blok zinciri ağını oluşturan herhangi bir terminaldir ve blok zincirine açılan kapılar olarak kullanılmaktadır. Kısaca, düğümler ağ katılımcılarıdır. Tipik bir blok zinciri ağında üç farklı düğüm türü vardır: basit (ligth), tam (full) ve madenci (miner). Ağdaki basit bir düğüm sadece işlemleri gönderip alabilmektedir. Bu düğümler defterin bir kopyasını saklamamaktadır, ayrıca işlem doğrulaması da yapmamaktadır. Tam bir düğüm ise bu işlemleri gerçekleştirmektedir. Madenci düğümü (blok oluşturucu), madencilik kabiliyetine sahip bilgisayarlardır, yani yeni bir blok oluşturma sürecine sahip tam bir düğümdür. Depolama bileşeni olarak çalışmakta, işlem kayıtlarının genel defterini saklamaktadır (Ismail ve Materwala, 2019).

Dağıtık Sistemler (Distributed Systems): Blok zinciri kilitli bloklar halinde paketlenmiş bir veri zincirini güvenli ve değişmeyen bir şekilde sıralı olarak depolayan dağıtılmış bir veri tabanıdır (Andrian vd. 2018). Bir DLT (Dağıtılmış Defter Teknolojileri - Distributed Ledger Technologies), dijitalleştirilmiş ve merkezi olmayan bir defterden oluşmaktadır. Düğüm adı verilen birbirine bağlı bağımsız bilgisayarlardan oluşan bir ağ gibi çalışmaktadır. Bu düğümlerin her biri ilgili defterlerinde gerçekleştirilen işlemleri gerçek zamanlı olarak paylaşmakta ve senkronize ederek çalışmaktadır (Abuelhija vd. 2020). DLT, bir defterin birden çok kopyasının oluşmasını sağlamaktadır. Birden fazla kopyanın diğer kriptografik protokollerle çiftler arasında dağıtılması, blok zinciri teknolojisinde gerekli değişmezliği sağlamaya yardımcı olmaktadır (Agbesi ve Asante 2019).

Defter (Ledger): Defter veya dijital defter, bir blok zincirinde blok oluşturan bireysel işlemleri içermektedir.

Blok (Block): Blok, bir işlemi depolayan bir veri yapısıdır. Defterdeki önceki bloğa bir referans içeren işlem kayıtlarını ve ek verileri barındıran veri yapısı olarak tanımlanmaktadır. Örneğin, bir günün satış işlemi veya bir beyanname sayfasına kaydedilen veriler blok zincirinin bir parçasını oluşturacak bloğa beslenen bir işlemi

temsil edebilmektedir. Bloklar, bir blok zincirinin bel kemiğidir ve birincil işlevi işlemlerin kaydedildiği yer olarak görülmektedir.

Genesis Blok: Genesis bloğu, blok zincirinin başlangıcıdır. Genesis bloğu genellikle yazılıma eklenmektedir ve önceki bir bloğa referans içermemesi açısından diğer bloklara göre farklılık göstermektedir. Bu blok, sistemde oluşturulan ilk geçerli blok özelliği göstermektedir (Sun vd. 2021). Blok içinde zincir konfigürasyonu, blok madenciliği için zorluk seviyesi gibi veriler yer almaktadır. Şekil 4.2'de örnek bir genesis blok ve değerleri gösterilmiştir.

- config: Dosya ağın temel işlemlerini kontrol eden tüm yapılandırma parametrelerini ve eşikleri içeren "config" bloğu ile başlamaktadır.
- chainId: Mevcut zinciri tanımlar ve tekrar (replay) koruması için kullanılmaktadır. Zincire özel benzersiz bir değere ayarlanması gerekmektedir.
- homesteadBlock: Homestead, Ethereum'un ikinci büyük sürümüdür (ilk sürüm Frontier'dir). 0 değeri, bu sürümün kullandığı anlamına gelmektedir.
- Zorluk (difficulty): Bu değer, ağda madencilik yapmanın ne kadar zor olduğunu belirlemektedir. Bir çalışma kanıtı oluşturmak için ne kadar hesaplama gerektiğini kontrol eden ağ genelindeki bir ayardır. Test ağında geliştirme yaparken, blok madenciliği için çok uzun süre beklemenize gerek kalmaması için bu değerin mümkün olan en düşük değere ayarlanması gerekmektedir.
- gasLimit: Bu değer, blok başına gaz maliyeti sınırını tanımlamaktadır. Bir işlemin veya bloğun tüketebileceği maksimum gaz miktarıdır. Test sırasında sınırlı kalmamak için bu değeri yüksek olarak ayarlanması gerekmektedir.

```
{
  "config": {
               "chainId": 15,
               "homesteadBlock": 0,
               "eip155Block": 0,
               "eip158Block": 0
              }

  "coinbase"   : "0x0000000000000000000000000000000000000001",
  "difficulty" : "0x10000",
  "extraData"  : "",
  "gasLimit"   : "0x4000000",
  "nonce"      : "0x0000000000000032",
  "mixhash"    : "0x0000000000000000000000000000000000000000000000000000000000000000",
  "parentHash" : 0x0000000000000000000000000000000000000000000000000000000000000000",
  "timestamp"  : "0x00",
  "alloc": {"7df9c865a174b3bc565e6424a1050ebc1b2d1d82": {     "balance": "10000"    },
            "f41b75c9ae680c1aa78f42e5647a62f353b7bdde": {     "balance": "20000"    }},
}
```

Şekil 4.2 Genesis Blok Yapısı Örneği

- nonce & mixhash: Nonce ve mixhash, birleştirildiğinde, bir bloğun gerçekten kriptografik olarak çıkarıldığını ve dolayısıyla geçerli olduğunu doğrulamaya izin veren değerlerdir. Mixhash, 64-bit nonce ile birleştirildiğinde, bu blokta yeterli miktarda hesaplamanın gerçekleştirildiğini kanıtlayan bir değer elde edildiği gösterilmektedir.Timestamp: Bu blok başlangıcında Unix time () fonksiyonunun makul çıktısına eşit bir skaler değer ile gösterilmektedir. Bu mekanizma, bloklar arasındaki zaman açısından bir uyuma zorlamaktadır. Son iki blok arasındaki daha küçük bir süre, zorluk seviyesinde bir artışa ve dolayısıyla bir sonraki geçerli bloğu bulmak için ek hesaplama gerekmesine neden olmaktadır. Periyot çok uzunsa, zorluk ve bir sonraki bloğa kadar beklenen süre azaltılmaktadır. Zaman damgası, zincir içindeki blok sırasının doğrulanmasına da izin vermektedir.

- Ayırma (alloc): Önceden doldurulmuş cüzdanların bir listesini tanımlamaya izin vermektedir. Her birinin ilk parametresi adresi göstermektedir.

- Ethereum Improvement Proposal (EIP); Ethereum topluluğuna bilgi sağlayan, önerilen yeni bir özelliğini, süreçlerini veya ortamını açıklayan bir tasarım belgesini ifade etmektedir.

Adres; bir blok zincirinde veya dağıtılmış defter ağında bir işleme katılan hesaplar için tanımlayıcı olarak kullanılmaktadır.

Nonce; Nonce, kriptografik bir hash'e eklenen özel bir sayıdır ve bu nonce, bir blok zincirindeki madencilerin blok zincirine yeni bir blok eklemek için çözmesi gereken sayı olarak ta kullanılmaktadır.

İşlem (Transaction); Bir blok zinciri ağındaki işlem, genel kayıtlarda saklanan küçük bir görev birimi olarak tanımlanmaktadır. Bu kayıtların blok zincirinde yürütülmesi ve depolanması, ağa dâhil olan katılımcıların çoğu tarafından önceden onaylanmasını gerektirmektedir. Daha önceki herhangi bir işlem, herhangi bir zamanda bir incelemeye tabi tutulabilmektedir ancak güncellenememektedir (Peters ve Panayi 2016, Sabry vd. 2019).

4.4 Özet Fonksiyonu (Hash Function)

Kriptografik özet fonksiyonu işlevi, güvenlik uygulamalarında yaygın olarak kullanılan bir mekanizmadır. Değişken boyutlu girdi verisini sabit boyutlu bir çıktıya dönüştüren matematiksel işlevdir. Çıktı, verilerin imzası olarak işlev gören, karma değer olarak adlandırılan bir şifreli metinden oluşmaktadır. Bu özellik, verilerin kendisini ifşa etmeden içeriğinin değiştiğini doğrulamak için kullanılabilmektedir (Paar ve Pelzl 2010). Bir bloktaki veriler değiştirildiğinde, özet değeri değişir ve bu da zincirdeki sonraki blokları etkilemektedir. Dolayısıyla, mevcut bir blokta değişiklik yapmaya yönelik herhangi bir girişim, sonraki bloklardaki bilgileri yanlış hale getirerek tüm blok zincirinin geçersiz olmasına neden olmaktadır. Kriptografik uygulamalarda yaygın olarak kullanılan birkaç popüler özet algoritması vardır. İyi bilinen algoritmalar MD5, SHA–1, SHA–256, Keccak256, RIPEMD 1'dir. Ancak bazı eski sürüm MD5 özet fonksiyonlarında olduğu gibi güvenlik açıklıkları

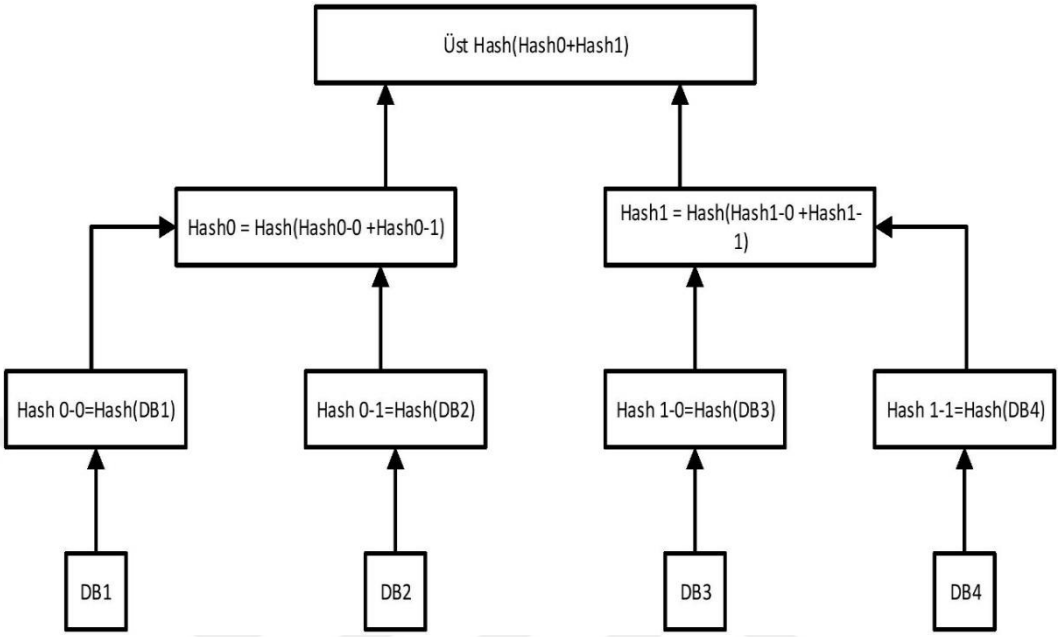
bulunabileceği belirtilmektedir. Çizelge 4.3'te bazı özet algoritmalarının uzunluk ve güvenlik seviyeleri belirtilmektedir (Shahzad ve Crowcroft, 2019).

Çizelge 4.3 Özet algoritmaları

Fonksiyon	Uzunluk	Güvenlik
Md5	128 bit	Hayır
RIPEMD 1	160 bit	Evet
SHA1	160 bit	Hayır
Keccak256	256 bit	Evet

4.5 Merkle Ağacı (Merkle Tree)

Madenci düğümler tarafından doğrulanan işlemler, daha sonra blok zincirinde bloklar halinde gruplandırılmaktadır. Bazen hash ağaçları olarak da anılan Merkle ağaçları tek bir blokta birden fazla işlemi toplamak için kullanılmaktadır. Bir Merkle ağacı, bir araya getirilen işlemlerin bütünlüğünü verimli bir şekilde özetleyebilmekte ve doğrulayabilmektedir. Aşağıdan yukarıya doğru oluşturulan işlem veri yapısı olarak tanımlanmaktadır. Orijinal verinin karması olan yaprak düğümlerden başlayarak, ilgili alt düğümlerinin bir bileşimi olarak üretilmektedir. Tek bir yaprak olmayan düğüm için, tüm alt düğümleri birleştirilmektedir. Sonuçta ağaçtaki düğümü temsil eden tek bir özet oluşturmak için karma hale getirilmektedir. Yaklaşım, kök düğüm olarak tanımlanan tek bir düğüm oluşturulana kadar devam etmektedir (Zaghloul vd. 2020). Çalışma prensibi Şekil 4.3'te gösterilmiştir. DB, veri bloklarını göstermektedir.



Şekil 4.3 Merkle ağacı (Geetha vd. 2021; Yan vd. 2020)

4.6 Akıllı Sözleşme (Smart Contract)

Sözleşme, piyasa ekonomisinin temel bir parçası olarak kullanılmaktadır. Hem işletmeler hem de bireyler arasındaki ilişkileri tanımlamaktadır. Akıllı sözleşme ise, bir sözleşmenin şartlarını kolaylaştırmak, yürütmek ve uygulamak için blok zinciri sistemi içinde çalışan yürütülebilir kod olarak tanımlanmaktadır. Akıllı sözleşmeler fikri, ilk olarak 1994'te Nick Szabo tarafından önerilmiştir (Alharby ve van Moorsel, 2017). Akıllı sözleşmenin temel amacı, belirtilen koşullar yerine getirildiğinde sözleşmenin şartlarını otomatik olarak yürütmektir. Akıllı sözleşmeler, merkezi olmayan sistemde kendi kendine yürütülen kod parçacıkları olarak geliştirilmektedir. Bu sözleşmelere gömülü işlevler, blok zinciri ağının en üst katmanındaki işlemlerin izlenmesine izin veren sözleşmelerini tanımlamaktadır. Blok zinciri ağındaki her düğüm, akıllı sözleşmeyi bağımsız olarak çalıştırarak bir fikir birliği ile doğrulaya bilmektedir (Abuidris vd. 2019). Akıllı sözleşmeler, sözleşmedeki içeriği belirli parametrelere göre gözden geçirerek uygulanmasını sağlayan süreç otomasyonuna izin vermektedir. Bu nedenle, akıllı sözleşmeler, güvenilir üçüncü tarafın

sözleşmenin şartlarını yürütmesini sağlamaktadır. Bu işlem takibi için geleneksel sistemlere kıyasla düşük işlem ücretleri ile işlemleri gerçekleştirebilmektedir (Shen ve Pena-Mora 2018).

Akıllı sözleşme programlaması, standart uygulama geliştirme yöntemlerinden farklı özellikler gerektirmektedir. Uygulamalarda herhangi bir problem varsa, hatalı yazılımın sonuçları özellikle finanslar işlemlerde çok yüksek maliyetli kayıplara sebep olabilmektedir. Beklenen değişikliklerin tüm sisteme tekrar yüklenmesi de zor olmaktadır. Genellikle akıllı sözleşme dilleri, ifadeler, operatörler, işlevler ve değişkenlerden oluşan ayrı bir programlama dilinde yazılmaktadır. Akıllı sözleşmenin çalışma süreci üç aşamada gerçekleştirilmektedir. İlk adım, akıllı bir sözleşme oluşturulması sürecidir. Solidity (Ethereum) veya Chaincode (Hyperledger) gibi yazılımlar geliştirme ortamı kullanılmaktadır. Solidity, C ++, Javascript, Python gibi diğer birçok üst düzey programlama diliyle aynıdır ve Ethereum Virtual Machine'de (EVM) akıllı sözleşmelerin uygulanmasında temel olarak geliştirme imkânı sağlamaktadır (Benita K vd. 2020). İkinci adım, akıllı sözleşmeyi dağıtmaktır, P2P ağı aracılığıyla her düğüme yayılır ve blok zincirinde belirli bir adreste bulunmaktadır. Akıllı sözleşmenin uygulanması üçüncü adımdır. Akıllı sözleşme, belirli koşullar sağlandığında otomatik olarak işlemleri gerçekleştirmektedir. Tüm yürütme sonuçları, geri döndürülemez ve izlenebilir işlemler olarak kaydedilmektedir. Akıllı sözleşmeler, merkezi olmayan bir ortamda yürütülebilen ölçeklenebilir uygulamalar olarak çalışmaktadır. Dağıtıldıktan sonra akıllı sözleşme kodu düzenlenemez veya yürütme davranışı değiştirilemez. Akıllı sözleşmelerin yürütülmesi, tarafların yazılı bir sözleşme için bir araya gelmesini garanti ettiği anlamına gelmektedir. Bu sayede, tek bir tarafa bağlı olmayan yeni, güçlü, güvene dayalı bir ilişki ortamı oluşturulmaktadır (Li vd. 2020).

4.7 Fikir Birliği / Uzlaşma Algoritması (Consensus Algorithm)

Tanım olarak fikir birliği, dinamik bir şekilde ulaşılan gruptaki anlaşmayı temsil etmektedir. Sistemin tutarlı ve hatasız çalışması, ayrıca kontrollerini sağlamak için

kullanılmaktadır. Düğümler arasında bir işlemin geçerli olduğu ve dağıtılmış defterde depolanacak işlemlerin bir sıralaması olduğu konusunda anlaşma olarak tanımlanmaktadır. İzinsiz blok zincirleri, işlemin sonucunda veriminden ödün verirken, hesaplama veya bellek karmaşıklığını kullanarak çok sayıda güvenilmeyen katılımcı arasında çok güçlü bir fikir birliği ortamı sağlamaktadır (Lone ve Mir 2019).

Blok zincirinde kullanılan farklı özelliklerde fikir birliği algoritmaları kullanılmaktadır, bunlardan bazıları iş ispatı (Proof of Work - PoW), teminat kanıtı (Proof of State - PoS), Bizans hata toleransı (Byzantine Fault Tolerant - BFT) veya Delegated Proof of Stake (DPoS) olarak belirtilmektedir. Bu tür fikir birliği mekanizmaları arasındaki temel fark, işlemlerin doğrulanmasındaki yetkilendirme ve ödüllendirme yöntemlerindeki değişiklikler olarak belirtilmektedir. Kararın oluşturulması, düğümler arasında belirli kurallar çerçevesinde belirli sayıda adımın atılmasıyla genel kabul esasına dayanmaktadır (Saad vd. 2019, Ferdous vd. 2020, Kaur vd. 2020). Bitcoin ve litecoin gibi en popüler kripto para ağları PoW fikir birliği algoritmasını kullanmaktadır (Saad vd. 2019a).

4.7.1 İş kanıtı (PoW Proof of Work)

PoW, blok zinciri platformları tarafından kullanılan en yaygın fikir birliği algoritması olarak bilinmektedir (Kaur vd. 2021, Sun vd. 2021). PoW, işlemlerin benzersiz ve güvenilir olarak doğrulanmasını sağlayan bir yöntem olarak kullanılmaktadır. Örneğin, blok zincirinde önceden belirlenmiş kurallara uyan bir hash oluşturmak için bloğun parçası olan ve belirlenen kriteri sağlayan nonce sayısını bulmaları gerekmektedir. Örneğin kural olarak özet değerinin altı sıfırla başlaması gerektiği şeklinde belirlenebilmektedir. Bu işlemin sonuçlarının doğrulanması ise kolay ve hızlıdır (Saad vd. 2019). Bununla birlikte, PoW'un dezavantajı maliyetli ve zaman alıcı bir süreç içerdiği belirtilmektedir (Lin ve Liao 2017). Madenciler bir Bitcoin blok zincirindeki ağa serbestçe girip çıkabildikleri için, mevcut zorluk seviyesi ile her iki bloğun madenciliği arasında 10’ar dakikalık bir aralık tutmak için ayarlanmaktadır. Buradaki doğrulama süreci merkezi olmamayı sağlamaktadır.

Matematiksel denklemlerin karmaşıklığı, blok madenciliğinin hızıyla orantılı olarak artırılıp azaltılmaktadır. Bu bir güvenlik önlemi operasyonu ve sömürü riskini azaltmanın bir yolu olarak kullanılmaktadır. Böylelikle bir blok zinciri veri madencilerinin oranına bağlı olarak formüllerin karmaşıklığını ayarlayabilmektedir Kararlı bir sistemi sürdürmek için denge öğesi olarak oluşturulmaktadır (Kaur vd. 2021). Başlangıçta, veri madenciliği mevcut grafik işlemci birimi kullanılarak kişisel bilgisayarlarda ki kaynaklar yardımıyla işlemler yapılabilmektedir. İşlem sayısı arttıkça ve blok zinciri büyüdükçe daha karmaşık hale gelmesi sonucunda, günümüzde daha yüksek performans gösteren özel donanımlı sistemlere ihtiyaç duyulmaktadır. Sonuç olarak işlemlerin tutarlılığını sağlayabilmek için çok fazla enerji tüketimine ihtiyaç duyan sistem ihtiyacı ortaya çıkmaktadır.

4.7.2 Teminat kanıtı (PoS – Proof of State)

Teminat kanıtı (PoS), blok zinciri ağında en çok tercih edilen uzlaşma algoritmalarından bir diğeridir. PoW'un aksine, doğrulayıcılar rastgele seçildikleri ve rekabet etmedikleri için önemli miktarda hesaplama gücü kullanmalarına ihtiyaç olmamaktadır. Sadece seçildiklerinde blok oluşturmaları ve önerilen blokları onaylamaları gerekmektedir (Leonardos vd. 2019). Bu algoritma PoW algoritmasına göre düşük maliyetli, düşük enerji tüketen bir alternatif olarak geliştirilen ortak fikir birliği algoritması olarak ortaya çıkmıştır. Bu protokolde, daha fazla varlığı olan kişiler doğrulama için kullanılmaktadır (Leonardos vd. 2019, Solat 2019). Sisteme dâhil edilen kripto paralar önceden oluşturulmuştur. PoW sistemlerinde olduğu gibi madencilik sürecine ihtiyaç duyulmamaktadır. Bu sayede karmaşık bir problem çözme işlemine, nonce değerini hesaplamaya ihtiyaç olmadığından daha hızlı ve yüksek enerji tüketimi olmamaktadır. PoS fikir birliği mekanizmasını kullanan en önemli platformlar Peercoin'dir (Kaur vd. 2021)

4.7.3 Delege edilen teminat kanıtı (DPoS- Delagated Proof of State)

PoS'ye benzer, ancak ağdaki düğümler delegeleri blok oluşturma ve doğrulama görevlerini yerine getirmesi için seçmektedir. Az sayıda seçilmiş delege ile çok hızlı

bir şekilde işlemler yapılabilmektedir. DPoS kullanan bloklar PoW veya PoS bloklarından daha hızlıdır. Burada küçük bir grubun doğrulama işlemlerini kontrol edebiliyor olması, sistemi merkezi hale dönüştürebilme ihtimalinin ortaya çıkarmaktadır. Temsilciler kötü niyetli olabilmekte ve gizlice birlikte çalışmaya başlayarak tüm ağda güveni tehdit edebilme ihtimali bulunabilmektedir (Luo vd. 2018, Wang vd. 2020).

4.7.4 Bizans hata toleranslı (BFT - Byzantine Fault Tolerant)

Düğümler arasındaki bazı farklılıklara rağmen hala koordine olabilen ve bir fikir birliğine varabilen uzlaşma protokolü olarak çalışabilmektedir (Gramoli 2020). Bizans hata toleransı, Bizans General Problemi olarak ta bilinen ve belirli bir hata sınıfının tolere edebildiği bir algoritmadır. Hyperledger bu algoritmayı kullanan en popüler izinli blok zinciri platformu olduğu bilinmektedir (Nasir vd. 2018). Hyperledger yapısında konsorsiyumlardaki katılımcı grubu bilinmektedir. Bu tür sistemler kimliklerin sistem içinde çalışan merkezi bir kayıt hizmeti ile kaydedildiği ve doğrulandığı bir konsorsiyum blok zinciri yapısı olarak çalışmaktadır (Shen ve Pena-Mora 2018, Lone ve Mir 2019). Hyperledger Fabric'te işlemleri, ağ ile etkileşime girecek uygulamaları yazma ve tasarlama yeteneği sağlayan programlama aracı olan zincir kodu (chaincode) kullanılarak geliştirilebilmektedir (Nasir vd. 2018).

PBFT (Practical Byzantine Fault Tolerant) ise BFT'nin farklı bir versiyonudur ve 1 / 3'e kadar Bizans düğümünü tolere edilebilir özellikleri olan bir algoritmadır. Konsensüs çalışmasında lider, diğer tüm düğümlere bir mesaj duyurmaktadır. Ardından dinleme aşamasına geçmektedir. Her düğüm liderden alınan mesajı kontrol etmektedir. Eğer doğrulama tamamlanırsa başkalarına iletilmektedir. Bir düğüm 2 / 3'ten fazla farklı düğümden aynı mesajı alırsa, çoğunluğun liderden aynı mesajı aldığından emin olunduğu sonucuna varılmaktadır. Böylece başkalarına onay mesajları gönderilmektedir. PBFT mekanizması, yalnızca küçük fikir birliği grubuyla iyi çalıştığı belirtilmektedir (Castro ve Liskov 2002, Gramoli 2020, Sun vd. 2021).

4.8 Şifreleme Yöntemleri

Verilerin gizliliğinin ve bütünlüğünün sağlanması önemli bir konu olarak ele alınmaktadır. Temel olarak verilerin gizliliğini ve bütünlüğünü sağlamak için simetrik veya asimetrik şifreleme yöntemleri kullanılmaktadır.

Simetrik şifreleme (Symmetric Encryption) Simetrik kriptografi, verileri şifrelemek için kullanılan anahtarın verilerin şifresini çözmek içinde kullanan yöntemdir. Dolayısıyla paylaşılan anahtar şifrelemesi olarak da bilinen bir kriptografi türünü ifade etmektedir. Kullanılan anahtar taraflar arasındaki veri alışverişinden önce oluşturulmalı veya üzerinde anlaşılarak dağıtılması prensibiyle çalışmaktadır. AES (Advanced Encryption Standard), DES (Data Encryption Standard), RC5 (Rivest Cipher 5) simetrik şifreleme yöntemlerinden bazılarıdır (Fontaine ve Galand 2007). Simetrik şifreleme algoritmaları daha az hesaplama gücü gerektirdiğinden daha hızlı çalışmaktadır. Ancak temel zayıflıkları anahtar paylaşımı olarak görülmektedir. Bilgileri şifrelemek ve şifresini çözmek için aynı anahtar kullanıldığından, bu anahtarın verilere erişmesi gereken herkesle paylaşılması gerekmektedir. Bu doğal olarak güvenlik riskleri oluşturmaktadır.

Asimetrik Şifreleme (Asymmetric encryption) Asimetrik kriptografi, verileri şifrelemek için kullanılan anahtarın, verilerin şifresini çözmek için kullanılan anahtardan farklı olduğu bir tür şifreleme anlamına gelir. Bu şemalarda farklı anahtarlar şifreleme ve şifre çözmede kullanılmaktadır. Bu anahtarlara genel/açık ve özel anahtarlar denilmektedir. Açık anahtar, şifreleme ve kimlik doğrulama için kullanılırken, özel anahtar şifre çözme ve imzalama için kullanılmaktadır. Asimetrik şifreleme sistemleri, simetrik sistemlere göre yavaştır ve daha uzun anahtarlar nedeniyle daha fazla hesaplama gücü gerektirmektedir. RSA (Rivest-Shamir-Adleman), DSA (Digital Signing Algorithm) ve El-Gammal gibi çeşitli asimetrik şifreleme şemaları kullanılmaktadır.

4.9 Dijital İmzalar

Dijital imza, dijital verilerin doğruluğunu ve bütünlüğünü doğrulamak için kullanılan kriptografik bir mekanizmadır. Süreç esas olarak, imzalayanın özel anahtarıyla birlikte bir mesaja özet fonksiyon uygulamaktan oluşmaktadır. Mesajın alıcısı, imzalayan tarafından sağlanan genel anahtarı kullanarak imzanın geçerli olup olmadığını kontrol edebilmektedir (Grontas ve Pagourtzis 2019). Çeşitli özelliklerde dijital imza uygulamaları kullanılmaktadır.

Kimlik doğrulama ve diğer özelliklerin ötesinde bir durumun işlevselliğini sağlayan birçok alternatif dijital imza şeması vardır. Bu dijital imza şemalarında, temel yöntemin sağlamadığı ek özellikleri elde etmek için belirli bir protokolle birleştirilerek farklı özellikte imza şemaları oluşturulmuştur. Bunlardan bazıları grup imza, halka imza, vekil imza ve eliptik eğri imzasıdır (Fang vd. 2020).

a) Çoklu İmza (Multi Signature); bir değerin belirli kişilerin onayı ile olması gerektiği durumlarda kullanılabilmektedir (Bellare ve Neven 2006, Xiao vd. 2021).

b) Grup İmzası (Group Signature); Chaum ve Heyst tarafından 1991 yılında tanıtılan grup imzaları yönteminde, imzalayanlar için anonimlik sağladığı belirtilmiştir. Grubun üyelerinden herhangi birisi iletileri imzalayabilmektedir. Bu yöntem ile imzalayarak imzalayanın kimliğinin korunduğu belirtilmiştir. Ancak ihtiyaç duyulursa kimin imzaladığının öğrenilmesinin de mümkün olduğu açıklanmıştır (Camenisch ve Michels 1998, Chaum ve van Heyst 1991).

c) Halka imzası (Ring signature); Rivest ve arkadaşları da, 2001 yılında grup imzadan farklı olarak, kullanıcının imzayı tam olarak hangi üyenin imzayı oluşturduğunu açıklamadan bir iletiyi imzalamasına olanak tanıyan farklı bir yöntem önermişlerdir. Bu imzalama yönteminde grup yetkilendirmesine ihtiyaç olmadığı belirtilmiştir (Bender vd. 2005, X. Li vd. 2020).

d) Vekil İmza (Proxy Signature) : Bir vekil imza protokolü, tanımlayıcı veya orijinal imzalayan olarak adlandırılan bir varlığın, geçici yokluk, zaman veya hesaplama gücü eksikliği vb. durumlarda, vekil imzalayan olarak adlandırılan başka bir varlığı kendi adına mesajları imzalaması için yetkilendirmesine izin verir. Temsilci imzalayan, orijinal imzalayanın sertifikalı ortak anahtarına erişimi olan herkes tarafından doğrulanabilecek bir proxy imzası hesaplayabilmektedir (Mambo vd. 1996, Boldyreva vd. 2003).

e) Eliptik Eğri İmzası (Elliptic Curve Digital Signature Algorithm - ECDSA) ; Bu yöntemde Bitcoin altyapında kullanılan bir yöntemdir. Ağıdaki Eliptik eğri fonksiyonu ile elde edilen grafik rastgele sayıların oluşturulması için kullanılmaktadır (Kontogiannis ve Varvarigou 2019, X. Li vd. 2020).

$$y^2 = x^3 + Ax^2 + Bx + C \quad A, B, C \in \mathbb{Z} \tag{4.1}$$

Bu eğri formülünde farklı parametrelerle farklı eliptik eğri dijital imzalar önerilmiştir. Bunlardan bazıları secp256k1 (Tan vd. 2019), Curve25519 (Salarifard ve Bayat-Sarmadi 2019) dir

RSA İmza, RSA şifreleme ile açık anahtar ve gizli anahtar oluşturması yönünden benzer özellikler göstermektedir. Ancak bu yöntemde mesajın özet fonksiyonu alınarak içerik imzalandığından içeriğin değişime uğrayıp uğramadığı da kontrol edilebilmektedir. Hesap işlemlerinde e (açık anahtar üs değeri), d (gizli anahtar üs değeri) ve n (modül) büyük asal sayı modül işlemlerinde kullanılmaktadır. Açık anahtar (n, e), Gizli anahtar (n, d) şeklinde oluşturulmaktadır. İmzalama aşamasında; mesajın özet değeri hesaplanıp özel anahtarla imzalanmaktadır. Özet fonksiyonu olarak SHA512 kullanılması önerilmektedir.

$$hsh = SHA512(msg), \qquad singnedMsg = hsh^d mod\ n \tag{4.2}$$

İmza doğrulaması aşamasında açık anahtarla içerik doğrulaması yapılabilmektedir. hsh ve hsh' eşitse imzalanmış verinin ve içeriğinin doğru olduğu kabul edilmektedir.

$$hsh = SHA512(msg), hsh' = singnedMsg^e mod\ n \qquad (4.3)$$

Bu bölümde açıklanan blok zinciri özellikleri uçtan uca kendi özel altyapının oluşturulması ihtiyacı olduğunda dikkate alınması gereken özellikler olarak dikkate alınmıştır. Özel bir Ethereum sistemi macOS, Linux ve Windows işletim sitemleri ile birlikte de çalışabilmektedir (Anonymous 2021). Bu tez kapsamında bu özellikleri uyarlayan bir test ortamı kurulmuştur. Bunun için Windows işletim sisteminde çalıştırılan bir özel Ethereum zinciri oluşturulmuştur. Lokal sistem için şekil 4.4'te belirtilen genesis özellikleri kullanılmıştır.

```
{  "coinbase"   : "0x0000000000000000000000000000000000000001",
  "difficulty" : "0x20000",
  "extraData"  : "",
  "gasLimit"   : "0x2fefd8",
  "nonce"      : "0x0000000000000042",
  "mixhash"    :
"0x0000000000000000000000000000000000000000000000000000000000000000",
  "parentHash" :
"0x0000000000000000000000000000000000000000000000000000000000000000",
  "timestamp"  : "0x00",
  "alloc": {},
  "config": {
      "chainId": 11,
      "homesteadBlock": 0,
      "eip155Block": 0,
      "eip158Block": 0
    }
}
```

Şekil 4.4 Ethereum test platformu Genesis.json dosyası

Ethereum alt yapısının uygulama geliştirme katmanı olarak kullanılan Visual Studio ile entegrasyonunda yaşanan problemler sebebiyle, blok zinciri uygulama geliştirme ortamı olarak önerilen Truffle alt yapısı kullanılmıştır (Truffle Suite 2021). Uygulamanın iki düğümlü test yayın ortamı içinde bulut çözümlerinin hizmetlere

kolay erişim ve kolay sistem yönetimi sunması nedeniyle (Bellini vd. 2019, Sathya vd. 2019), Azure bulut blok zinciri sistemleri kullanılmıştır. Bulut sistemlerinin sağladığı bazı avantajları olmuştur. Sistem düğüm sayısının ve kaynaklarının ihtiyaca göre artırılabilmesi en önemli faydalarından biri olmuştur. Ancak 3 yıldır kullandığımız bulut servisi hizmetini sağlayan Microsoft şirketi 10 Eylül 2021 tarihinde bu servisi durdurma kararı almıştır (Microsoft 2021). Bu durum gerçek bir sistem tasarımda dikkate alınması gereken en önemli kriterler arasında değerlendirilmesi gerektiği kanaatini oluşturmuştur.

5. SİSTEM TANIMLAMASI

Bir bütün olarak seçim sisteminin devreye alınması çok uzun ve karmaşık süreçleri içermektedir. Bu nedenle araştırmada dikkate alınan bazı varsayımlar olmuştur.

a) Tüm seçmenlerin doğru listelendiği, biyometrik kimlik kartına sahip olduğu ve kimlik doğrulamasının bağımsız cihazlarla yapıldığı kabul edilmiştir.

b) Seçmen iyi eğitimlidir ve temel haklarının ve seçim sürecinin farkındadır. Her seçmenin öngörülen sürede oy verebilmesi önem taşımaktadır.

c) Tüm seçmenlerin kayıt sırasında problemsiz bir şekilde şifre belirlemeleri ve sonrasında da tokenlarını kaybetmedikleri varsayılmaktadır.

d) Bağlantının her zaman mevcut olduğu ve iletişim gecikmesinde herhangi bir gecikme yaşanmadığı ve internetin kesintiye uğramadığı varsayılmaktadır.

e) Ayrıca seçim görevlilerinin teknolojiden haberdar olduğu ve seçmenlere rehberlik edebilecekleri varsayılmaktadır.

f) Büyük bir seçim alt yapısını oluşturmanın zorluğu sebebiyle, sınırlı kaynak kullanımı yapılarak test ortamında tasarlanmıştır.

Blok zinciri teknolojisinin merkezi olmama ilkesi, seçimlerin bütünlüğünü ve farklı kuruluşlar tarafından kontrol edilebilirliğini artırabilmektedir. Blok zinciri tabanlı oylama tasarımı, her oy pusulasının sürekli olarak, her veri girişini birden fazla düğüm boyunca kaydetmeye dayanmaktadır. Önerilen sistemde güvenli konsorsiyum bir ağ altyapısı ve akıllı sözleşmeleri kullanabilen Ethereum blok zinciri kullanmaya karar verilmiştir. Ethereum tabanlı test platformunun kurulum aşamaları Google Drive linkinde "EK1.BlokzinciriTestPlatformuKurulumu.docx" dosyasına yüklenmiştir. İndirmek için linki kullanabilirsiniz. Test platformu için geliştirilen uygulama Ganache / Trufle platformu üzerinde çalıştırılmıştır. Sistemin tasarım ekranlarında kullanılan verileri için MS SQL 2016 veri tabanı kullanılmıştır. Seçim sisteminde kullanılan tabloların SQL scripti Google Drive

"EK2.VeritabanıScripti.docx" dosyasına yüklenmiştir. Tüm dosya yazılımı ve kaynak dosyalarını Google Drive linkinden indirebilirsiniz.

Sistem tasarımlarında kullanılan sistemlerin özellikleri çizelge 5.1'de listelenmiştir.

Çizelge 5.1 Sistem tasarımında kullanılan sistemlerin özellikleri

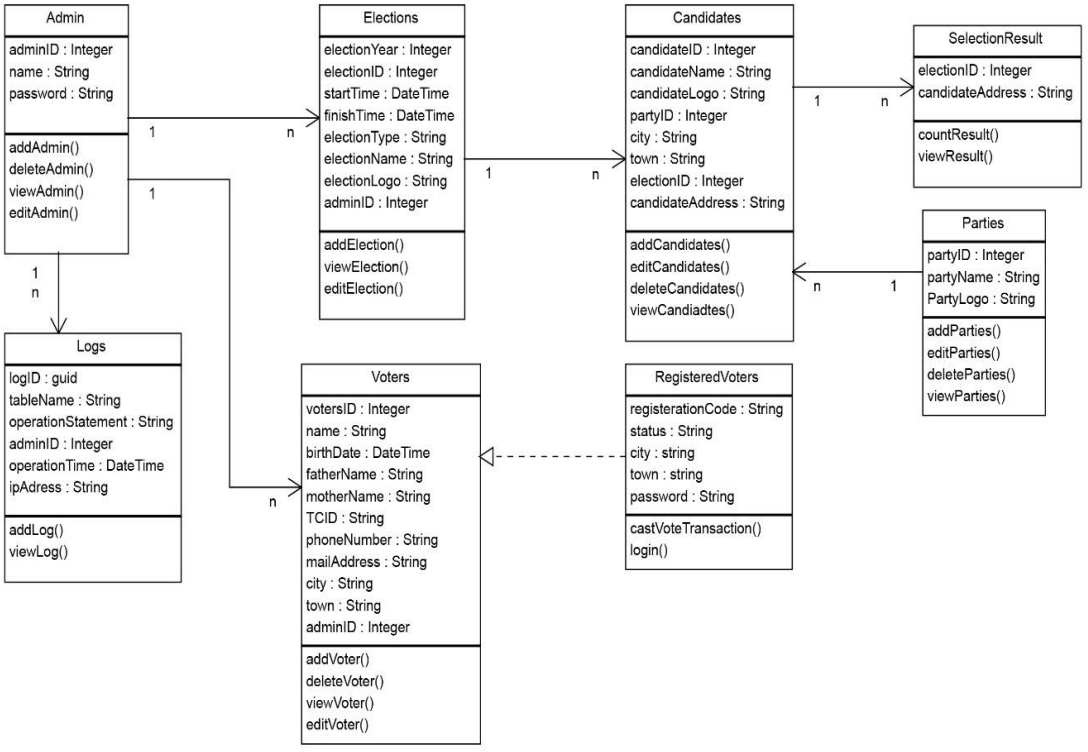
Özellik	**Lokal Test**	**Bulut Test**
Geliştirme Ortamı	Visual Studio 2015 asp.net, C sharp	Visual Studio 2019 asp.net, C sharp
Akıllı Sözleşme Geliştirme	Visual Studio Code + Solidity plugin	Visual Studio Code + Solidity plugin
Blok zinciri Altyapısı	Truffle Ganache 2.0 Ethereum	Azure Ethereum Servisi
Uygulama Sunucu Özellikleri	Windows Server 2019 x64 Internet Information Services 10 Intel Xeon CPU E5 2699 2.20 GHz (8 İşlemcili) 12 GB RAM	Azure Uygulama Servisi
Düğüm Sayısı	1	2
Kullanıcı Sayısı	100	Seçmen Sayısı Kadar

Seçim sürecinde farklı ihtiyaçlar ortaya çıkabilmektedir. Seçime hazırlık hizmeti birimi seçmen listeleri, adaylar, seçim tipi ve süreçlerinin belirmesine yardımcı olmaktadır. Seçmen kaydı oluşturulurken oy kullanmaya uygun kişilerin doğrulanması ile ilgili süreçler belirlenmelidir. Ayrıca seçmenlerin seçimden önce kayıt yaptırmaları gerekmektedir. Seçim tamamlandıktan sonra da otorite sayım işlemlerini doğrulayarak, sonuçları açıklamakla yükümlüdür.

Yukarıdaki bilgilere dayanılarak kavramsal bir model oluşturulmuştur. UML (Unified Modeling Language) sınıf diyagramı modeli, e-oylama uygulaması geliştirmenin tasarım ve uygulama aşamalarında temel olarak kullanılmıştır (Şekil

5.1). UML sınıf diyagramı, çeşitli sınıflar ve bunların özellikleri arasındaki ilişkiyi göstermektedir.

Yönetici, bir seçimi yönetmekten sorumlu kişi olarak tanımlanmaktadır. Yönetici seçim tarihini, süresini, seçim türünü ve adayları hazırlamakla yükümlüdür. Seçim sınıfın da ise seçim günü, süresi ve diğer ilgili bilgileri saklanmaktadır. Bu yapı sayesinde sistemin farklı seçimlerde de kullanmak için esneklik içermesi sağlanmış olmaktadır. Yöneticinin temel görevlerinden biri de seçmenlerin ve kayıtlı seçmenlerin listesini hazırlamaktır. Seçmenler ve kayıtlı seçmen sınıfları, kimlerin oy kullanabileceğini, seçim otoritesinin belirlediği kriterlere uygun olarak hazırlamaktadır.



Şekil 5.1 E-oylama sisteminin kavramsal UML sınıf diyagramı

Sürecin verimli olabilmesi için, seçmenin sisteme erişebilmesi ve kimlik doğrulaması yapabilmesi için bir kimlik numarasına, bazı kişisel bilgilere veya gizli anahtara sahip olması gerekmektedir. Kayıt sırasında seçmenlere oy kullanabilmeleri için gizli

kodlar oluşturmaları sağlanmalıdır. Seçim günü oy verme hakkı olan vatandaşlar bu kodları kullanarak seçimlerde oy kullanabilmelidir.

Yönetici tarafından gerçekleştirilen tüm işlemlerin günlük kayıtlarını tutmanın yanı sıra, seçim sonuçlarının güvenli bir şekilde saklanması da çok önemlidir. Bu aşamada, Ethereum tabanlı blok zincir sistemleri, oyların saklanması için tasarlanmıştır. Ayrıca sistem tasarımına göre akıllı kontratlarda gerekli kontroller ile sisteme dâhil olan düğümler senkronize edilerek dağıtık yapıda çalışması sağlanabilmiştir. Ayrıca otoriteler seçim sonucunu sağlıklı bir şekilde sayımından da sorumlu olduğundan bu konuda da güvenilir ve şeffaflığı sağlamak için dağıtık yapıda katılımlı sonuç belirleme yöntemi kullanılmıştır. Çizelge 5.1'de belirtilen uygulamanın bulut ortamı testleri için Azure Ethereum oluşturma aşamaları Google Drive linkine (EK3.BulutBlokzinciriKurulumu.docx) yüklenmiştir.Akıllı sözleşmeler tüm oylama katılımcıları için görünür ve şeffaf olduğundan, hassas verilerin depolanması için uygun olmadığı belirtilmektedir. Bu nedenle sistemimizde gizlilik özellikleri nedeniyle homomorfik şifreleme tercih edilmiştir.

5.1 Homomorfik Şifreleme

İlk olarak 1978 yılında önerilen homomorfik şifreleme teknikleri (Rivest vd. 1978), veri işleme alanında, özellikle bulut bilişim alanında önemli ilerlemelere yol açmıştır. Homomorfik şifreleme, orijinal verilerle yapılmak istenilen bazı işlemleri, şifrelenmiş verilerin şifresini çözmeden doğrudan şifrelenmiş veriler üzerinden yapılmasına imkân veren bir şifreleme yöntemidir (Balasubramanian ve Jayanthi, 2016). Homomorfik şifreleme Kısmen Homomorfik Şifreleme (PHE – Partially Homomorphic Encryption), Biraz Homomorfik Şifreleme (SHE – Somewhat Homomorphic Encryption) ve Tam Homomorfik Şifreleme (FHE – Fully Homomorfic Encryption) (Shrestha ve Kim 2019, Kim ve Yun 2021,).

a) Kısmi Homomorfik Şifreleme (PHE): PHE şemasında, şifrelenmiş mesaj üzerinde yalnızca bir tür matematiksel işleme, yani sınırsız

sayıda toplama (Cominetti ve Simplicio, 2020) veya çarpma işlemine izin verilmektedir (K. Peng vd. 2004).

b) Biraz Homomorfik Şifreleme (SHE): SHE'de hem toplama hem de çarpma işlemine izin verilir, ancak yalnızca sınırlı sayıda işlem yapılabilmektedir (Cheon ve Kim 2015).

c) Tam Homomorfik Şifreleme (FHE): FHE, şifreli mesaj üzerinde sınırsız sayıda çok sayıda farklı türde değerlendirme işlemine izin verilmektedir (Gentry 2009, Saproo vd. 2020).

Homomorfik özellikler gösteren bazı algoritmalar çizelge 5.2'de listelenmiştir. Örneğin, yarı homomorfik bir şifreleme tekniği olan Paillier yöntemi (Paillier 1999), şifreli verilerle yapılan işlemler neticesinde toplamının hesaplanmasına izin vermektedir. Aksine, ElGamal şifrelemesi (ElGamal 1985), şifrelenmiş verilerin çarpımı kullanılarak düz verilerin çarpımı elde edilebilmektedir. Buna karşılık, Boneh Goh Nissim 'nin şifrelemesi (Boneh vd. 2005) gibi tamamen homomorfik şifreleme şemaları, şifrelenmiş veriler üzerinde uygun aritmetik işlemler yoluyla düz verilerin hem çarpılmasına hem de toplanmasına izin vermektedir.

Çizelge 5.2 Homomorfik özellik gösteren algoritmalar

Algoritma	**Homomorfizm**
RSA (Rivest vd. 1978)	Çarpım
Pailler (Paillier 1999)	Toplama
ElGamal (Elgamal 1985)	Çarpım
Boneh Goh Nissim (Boneh vd. 2005)	Toplama ve Çarpım

Homomorfik şifreleme, gizli bilgileri bilgisayar sistemi içinde güvenli bir şekilde iletmek ve saklamak için bir araç olarak kullanılabileceği belirtilmektedir (Ogburn vd. 2013). Medikal uygulamalarda, biyometrik verilerin yüksek hassasiyeti sebebiyle herhangi bir bilgi sızıntısında ciddi bir gizlilik tehdidi oluşturabileceğinden, bu tür

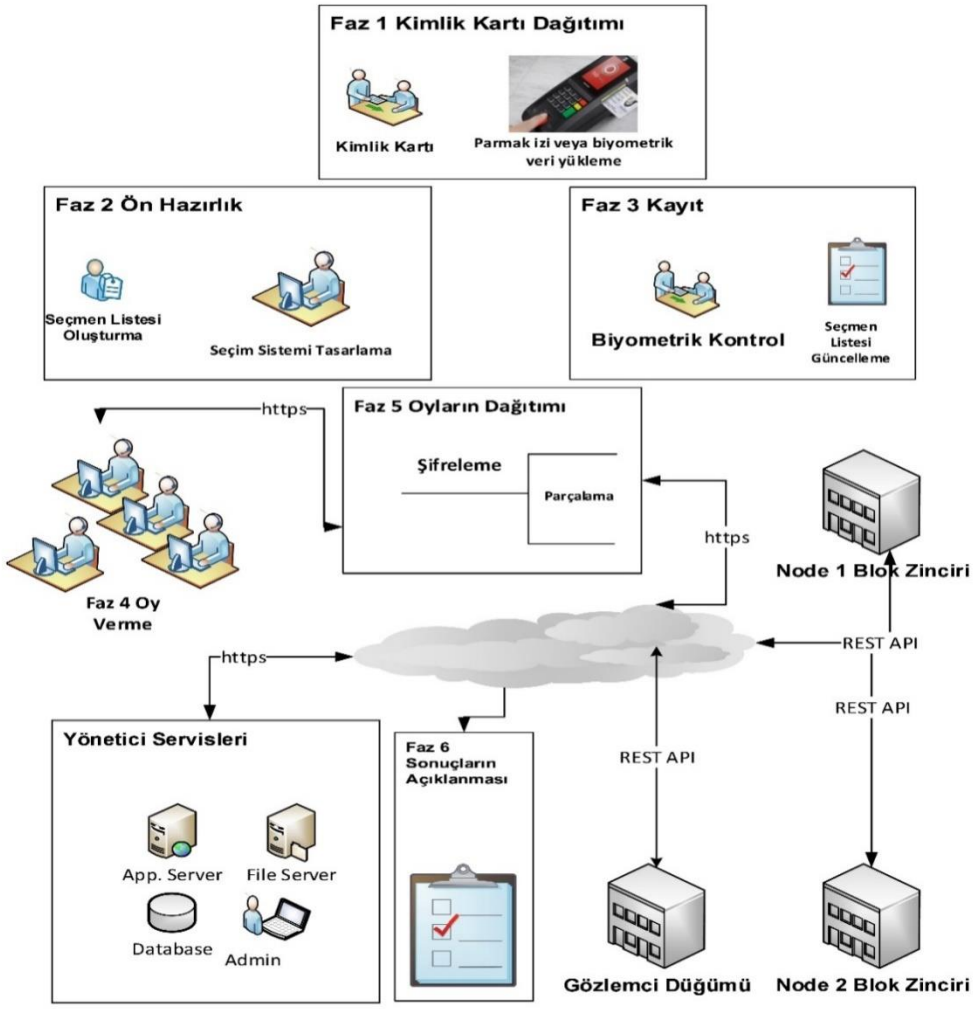
verilerin paylaşılmasında (Dowlin vd. 2017, Gomez-Barrero vd. 2017) , finans (Peng vd. 2016), forensik resim gibi farklı alanlarda kullanılabileceğine yönelik araştırmalar ve öneriler yer almaktadır (Alaya vd. 2020). Homomorfizm özelliği ise şifreli içeriklerin şifresini çözmeden çalışmasına izin vermesi açısından anonimlik sağlamak için yardımcı olmaktadır (Balasubramanian ve Jayanthi 2016, Yu vd. 2018). Özellikle son zamanlarda bulut servislerinin yaygınlaşması ile verilerin gizliliği çok daha fazla önemli bir hale gelmeye başlamıştır. Microsoft firmasının da homomorfik şifrelemeye yönelik SEAL Kütüphanesini bu tür kullanımlar için paylaşılmıştır (Microsoft Seal 2021).

Sistemde kullanılan şifre yöntemi değerlendirildiğinde; klasik şifreleme yöntemlerinden farklı bir şifrelemeye ihtiyaç duyulmuştur. Genellikle klasik şifreleme yöntemleri veri saklama amacıyla kullanılmaktadır. Bu yöntemlerle yapılan şifreleme sonucunda, herhangi bir işlem yapılmak istendiğinde içeriğin çözümlenmesine ihtiyaç duyulmaktadır. Oylama sitemlerinde ise kullanılan oyun içeriğinin ifşa olmaması en önemli unsurlardan birisidir. Bu sebeple tercih ettiğimiz şifreleme yöntemi sayesinde seçim sisteminde kullanılan oylar şifrelenerek gerekli veri gizliliği ve anonimlik sağlanmıştır. Tercih edilen şifreleme yöntemi ile şifreli verilerin çözülmeden de sonuçların sayım işleminin gerçekleştirilebilmesi sağlanmıştır. Ayrıca klasik şifreleme yöntemleri ile aynı veri için aynı sonuç elde edilmektedir. Bu durumda da şifreli veriler üzerinden sonuçları kategorize edebilmesi riskini oluşturmaktadır. Bu riski ortadan kaldırmak için kullanılan yöntemde aynı tercih için farklı şifrelenmiş veri elde edilmesi sağlanarak, bu kez de aynı tercih için farklı sonuç elde edilmesi sağlanmıştır. Önerilen sistemde ayrıca; hassas oylama verilerinin korunması için homomorfik şifreleme sonrası elde edilen verilerin parçalanması ve dağıtılması da önerilmiştir. Gizli veri paylaşımı, dağıtılmış ağlar arasında önemli bilgi parçalarını güçlü bir şekilde dağıtmak için kullanılan bir tekniktir. Bu nedenle ikinci güvenlik katmanı olarak Shamir Gizli Paylaşım yöntemi entegrasyonun uygulanması tercih edilmiştir (Shamir, 1979). Bu sayede uygulanan

homomorfik şifreleme yeteneklerine ek olarak, hem verilerin yedekliliği hem de çapraz kontrol özellikleri elde edilmiştir.

5.2 Oylama Modeli

Önerilen sistemin şeması ve önerilen algoritma şekil 5.2 ve şekil 5.3'de gösterilmiştir. Her aşamada yapılması gereken sistem prosedürleri aşağıdaki süreçleri kapsamalıdır.



Şekil 5.2 Blok zinciri oylama modeli

a) Faz 1: Kimlik Dağıtımı; Parmak izi veya biyometrik verilerin yüklü olduğu kimlik kartlarının her vatandaşa dağıtımı zamanı geldiğinde eksiksiz tamamlanmalıdır (Şekil 5.2).

Girdi: Voter ID

Çıktı: Parçalanmış Veri

```
Begin
If Voter Id in Voter List Id then // Seçmen kontrolü
    Get the voter Token, set the password
else not an eligible voter exit
if (voter Id in registered voter list) then //Kayıtlı seçmen kontrolü
    Check Token and Password
else not registered voter exit
if not voted (token and password) then
    chose Candidate ID
    chipherData = HomomorphicEnc (Candidate ID) // veri şifreleme
    chiperBallot= SecretShareSlicer (chipherData) // veri parçalama
    send chiperBallot to blockchain nodes //blok zincirine transaction başlatma
else failed login exit
END
```

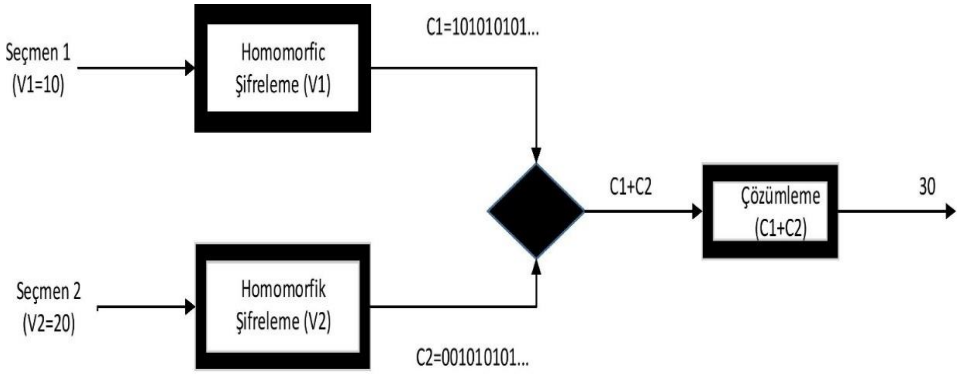
Şekil 5.3 Oy verme algoritması

b) Faz 2: Ön hazırlık aşaması genellikle verilerin (seçim süresi, adayların belirlenmesi, seçim bölgeleri gibi) oluşturulması, seçmen listelerinin hazırlanması süreçleri ile ilgili olmaktadır. Seçmenler

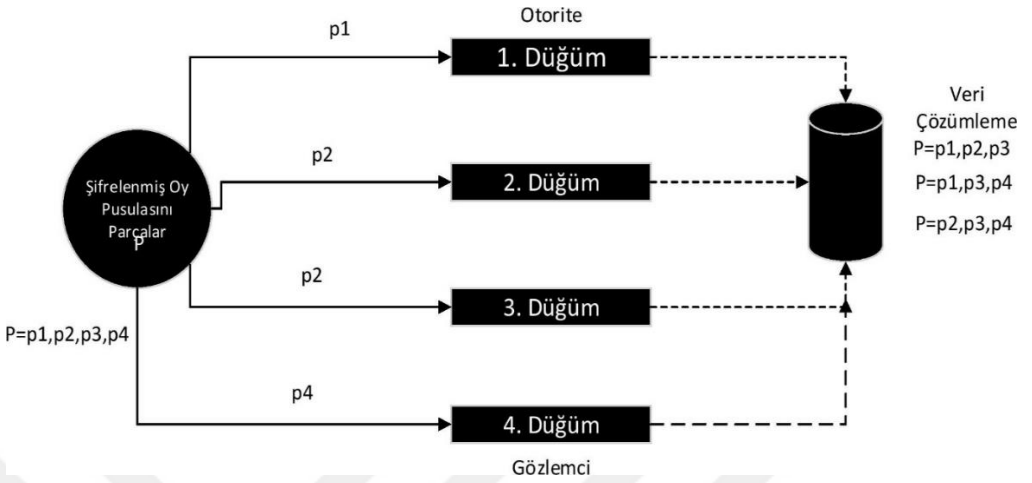
uygun kriterler doğrultusunda seçim komisyonu tarafından belirlenerek oluşturulmalıdır. Daha sonra bu veriler seçim öncesinde oluşturulan bürolardaki kayıt esnasında güncellenmelidir.

c) Faz 3: Kayıt; Seçmenler, parmak izi / biyometrik veri içeren kimlik kartı ile oy kullanma bürolarına başvurmalıdırlar. Bu veriler bağımsız özel bir cihaz yardımıyla kontrol edilmelidir. Oylama hizmeti ofisi yöneticisi, kişinin oy kullanma hakkını bir kez de sistemdeki kayıtlar üzerinden kontrol etmelidir. Yetki verilmişse kapalı zarf içinde token seçmesi yaptırılarak, şifre belirlemesi sağlanmalıdır (Şekil 5.2).

d) Faz 4: Oylama; Oy kullanmaya yetkili olan seçmenlerin kontrolü yapılarak seçim sistemine girişlerine izin verilmelidir (Şekil 5.7). Oy kullanan seçmenlerin listesi otomatik olarak oy kullandı olarak güncellenmelidir. Sistemin interaktif ara yüzler aracıyla sunduğu ara yüzlerden tercihini yapması sağlanmalıdır.



Şekil 5.4 Oy pusulası şifreleme, homomorfik toplama örneği



Şekil 5.5 Şifreli veri parçalı dağıtımı örneği

e) Faz 5: İşlem; Blok zinciri altyapılarında veriler tüm paydaşlarda açık olarak takip edilmektedir. Anonimlik, verilerin ifşasını önlemek ve çapraz kontrol sağlayabilmek için, bu aşamada tercih ilk olarak homomorfik şifreleme ile şifrelenmektedir (Şekil 5.4), daha sonra parçalara ayrılmaktadır (Şekil 5.5). Ardından, işlemlerin tüm düğümlere aktarılması süreci başlatılmaktadır (Şekil 5.7).

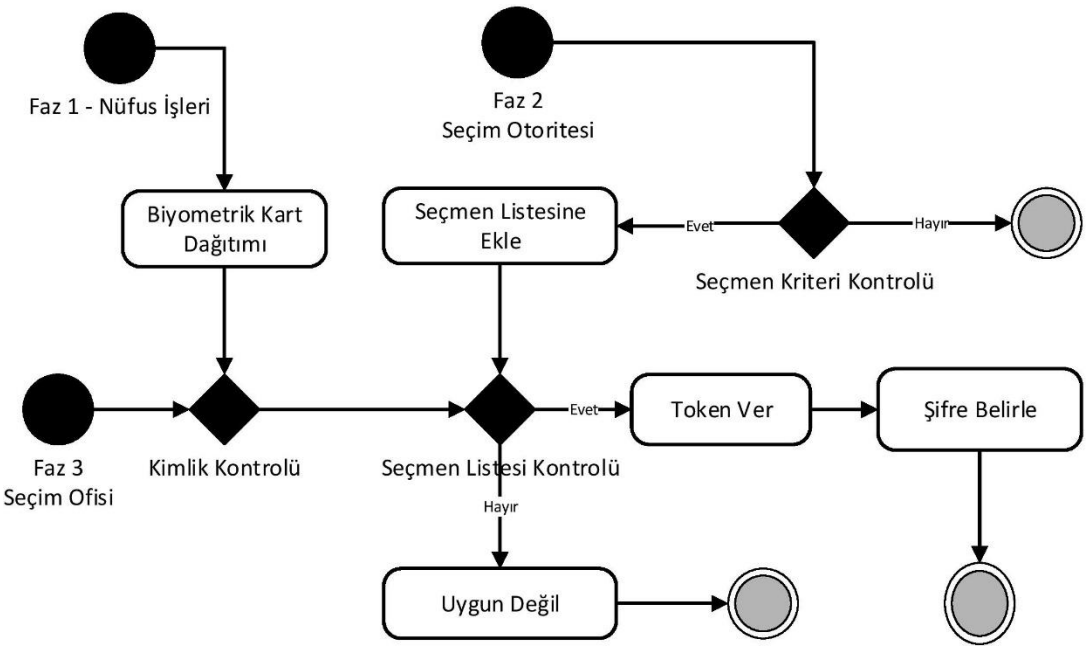
f) Faz 6: Sayım; Bu aşama, oy sayma görevlerini, sonuçları analiz etmeyi ve son olarak kazananları ilan etmeyi içermektedir (Şekil 5.10). Sayım sonuçlarını elde edebilmek için verileri birleştirme işlemini tamamlamak üzere bir araya gelen düğümler, önce parçalanmış verileri birleştirmekte, sonrasında da sayımı gerçekleştirmektedir. Diğer düğümler çapraz kontroller yaparak sonuçları doğrulayabilmektedir. Tüm kontrollerde aynı sonuçların elde edilmesi gerekmektedir.

Önerilen sistemin akış şemasında gerçekleştirilen işlemler şekil 5.6 ve şekil 5.7'de gösterilmektedir. Süreçlerde yer alan sorumluların görevleri çizelge 5.3'te özetlenmiştir. İlk aşamada her vatandaşa (Ci) Biyometrik Kimlik kartı verilmelidir. Gerekli tüm bilgiler çip kartlara yüklenmelidir. Seçim sistemi gerekliliklerinden

Seçim Yönetim Kurulu sorumludur. Sistem yöneticileri, seçim yetkilileri, sistem parametrelerini başlatarak ve bir seçimin farklı aşamalarını tetikleyerek oylama sürecini organize ederek ve kontrol edecektir.

Çizelge 5.3 Seçim organizasyon birimleri

Sorumlu / Birimler	**Görevi**
Seçim Yönetim Kurulu, Seçim Otoritesi	Seçim sisteminin sahibidir. Seçim sürecini yönetmektedir. Seçmen Listesini oluşturur.
Nüfus İşleri	Kimlik dağıtımını gerçekleştirir
Sistem Geliştirme Yöneticisi	Sistem tasarımı, akıllı sözleşme geliştirmesi, testleri ve geliştirme süreçlerini yönetir, seçim otoritesine raporlar.
Seçim Kayıt Sorumlusu	Seçmen Kayıt işlemlerini yönetir.
Seçim Ofis Sorumlusu	Seçmenlerin kontrolünü sağlar.
Seçmen	Oy verme işlemlerini gerçekleştirir
Gözlemci	Seçim sonuçlarını doğrular



Şekil 5.6 Kart dağıtımı, kayıt fazları iş akış diyagramı

Seçim otoritesi kritere uygun kişilerden (Ci) seçmen listesini (Vi) oluşturmalıdır.

$$Vi \leftarrow Ci \tag{5.4}$$

Çizelge 5.4 Sistem parametreleri

Sistem Parametreleri	**Tanım**
Ci	Seçmen
Eid	Seçim kimlik no
RegOfficeID	Seçim ofis kimlik no
CLi	Aday kimlik no

Seçim otoritesinin belirlediği çizelge 5.4 seçime özel sistem parametrelerine (Adaylar, seçmeler, seçim ve seçim büro tanımlamaları vb.) uygun olarak seçim sistemini tasarlamakla görevlidirler. Tüm sistem bileşenlerinin kontrollerin bağımsız birimler tarafından da test edilmesi gerekmektedir.

Kayıt büroları seçmenlerin doğruluğunu sağlayıp seçmen listelerinin güncellenmesinden sorumludur.

$$\text{updateVoterList}\ (Ci) \tag{5.5}$$

Doğrulama sonrası seçmenlere token dağıtımı yapılmalıdır. Bu tokenlar bir kez kullanılabilmelidir. Seçim gününde yine doğrulama sonrası bu tokenlar yardımıyla oylama yapma imkânı sağlanmalıdır. Seçmenin başkasının token bilgisi ile oy kullanımını engellemek için kayıt sırasında farklı bir blok zinciri / veri tabanı üzerinde kayıtlı seçmenlerin kimlik numaraları/biyometrik bilgileri saklanmalıdır.

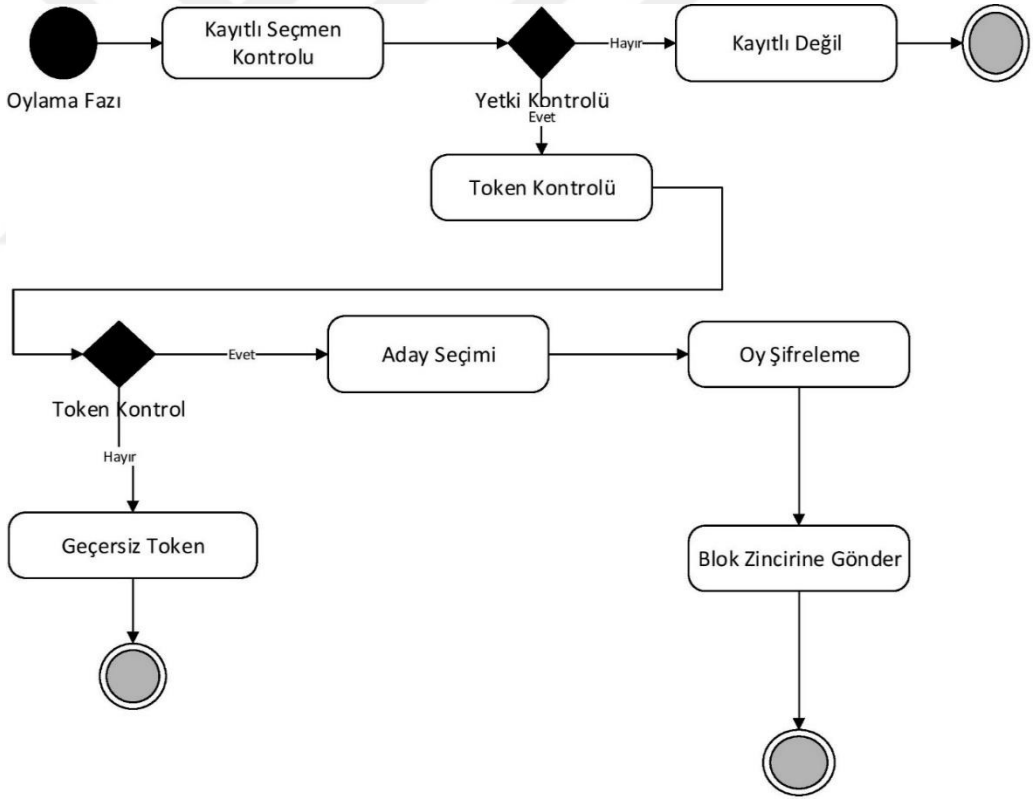
Seçmenin uygun adayı belirlemesinden sonra oy pusulasının şifreleme işlemleri başlatılıp gönderilmesi süreçleri başlatılır. Oy vermeye yetki kontrolünü geçen seçmenleri oy kullandıkları sisteme girilmelidir. Bu süreçler şekil 5.4 ve şekil 5.5 ‘de gösterilmektedir. Önce Homomorfik şifreleme sonrasında da bu şifreli metnin parçalara ayrılarak düğümlere dağıtılması aşaması başlatılmış olmaktadır.

$$Encrypted\ ChipherBallot \leftarrow SecretShareSlicer\ (HomomorphicEnc\ (CLi)) \tag{5.6}$$

Bu oy pusulası, oylama aşamasında tüm blok zinciri düğümlerine dağıtılmaktadır. Gönderilen işlem verileri geçerliyse blok zincirine eklenir (Şekil 5.7).

$$SendBallotTransaction\ (Token, ChipherBallot, Eid, RegistrationOfficeID, timestamp, Pubkey) \tag{5.7}$$

Oy şifreleme aşamasını (Şekil 5.4 ve Şekil 5.5), biçimsel olarak uygulanan yöntemlerin önemli parametrelerini şu şekilde özetleyebiliriz.



Şekil 5.7 Oy verme fazı iş akış diyagramı

p ve q rastgele asal sayı olarak seçilir, n bu değerlerin çarpımı olarak hesaplanır.

$$n = p.q \tag{5.8}$$

$$\lambda(n) = \text{lcm}\,(p-1, q-1)$$
(en küçük ortak bölen, lcm) (5.9)

Şayet p ve q aynı uzunlukta seçilirse generator $g = n + 1$ şeklinde seçilebilir veya rastgele $g \in Z^*_{n^2}$, $\gcd(g, n^2) = 1$ seçilebilir. n ve g açık , p ve q özel olarak paylaşılmaktadır. x mesajı, seçim yapılan adayın sayısal değerle ifadesini, y ise bu değere karşılık gelen şifrelenmiş mesajı göstermektedir. r değeri rastgele seçilen bir değerdir, şifrelenmiş verilere farklılık kazandırmaktadır.

$$0 < r < n\,, \qquad r \in Z^*_n \tag{5.10}$$

Şifreleme işlemi; seçim değeri (x) ve rastgele değerle (r) aşağıdaki gibi hesaplanmaktadır.

$$y = Enc(x, r) = g^x . r^n mod\ n^2 \tag{5.11}$$

Çizelge 5.5 Seçilen değerin şifrelenmesi örneği

Vote	**A** 2^4	**B** 2^2	**C** 2^0	**x**	**Random Number r**	$Enc(x,r) = g^x . r^n mod n^2$ **g= n+1, n^2**
1	x			16	131	$Enc(16,131)$
2		x		4	161	$Enc(4,161)$
3			x	1	83	$Enc(1,83)$
4	x			16	160	$Enc(16,160)$
5		x		4	62	$Enc(4,62)$
6	x			16	81	$Enc(16,81)$
7			x	1	135	$Enc(1,135)$

Çizelge 5.5 bu duruma uyan örnek seçim ve rastgele değerlerle elde edilen şifreli değerleri göstermektedir. Burada önemli unsur aynı tercih yapılsa bile elde edilen

şifreli metinin rastgele seçilen değer yardımıyla farklı elde ediliyor olmasıdır. Sistemin geliştirme ortamındaki simülasyonları için geliştirilen uygulama "CloudTestApplication_TRTVotingWeb.rar" dosyası Google Drive sistemine yüklenmiştir. Bu sıkıştırılmış dosya içinde yer alan "HomomorphicEncryption.aspx" dosyası homomorfik şifreleme simülasyonu için kullanılmıştır.

Tüm oylar $Enc(x,r)$ çarpılıp Modulo n^2

$$Tüm\ Oylar \coloneqq \prod Enc(x,r)\ mod\ n^2 = y\ mod\ n^2 \tag{5.12}$$

$$x = Dec(y) = \frac{L\ (y^{\lambda}\ mod\ n^2)}{L\ (g^{\lambda}\ mod\ n^2)} mod\ n \tag{5.13}$$

$$L\ (u) = \ (u-1)/n \tag{5.14}$$

$$L1 = \ L\left(y^{\lambda}\ mod\ n^2\right) \tag{5.15}$$

$$L2 = \ L\left(g^{\lambda}\ mod\ n^2\right) \tag{5.16}$$

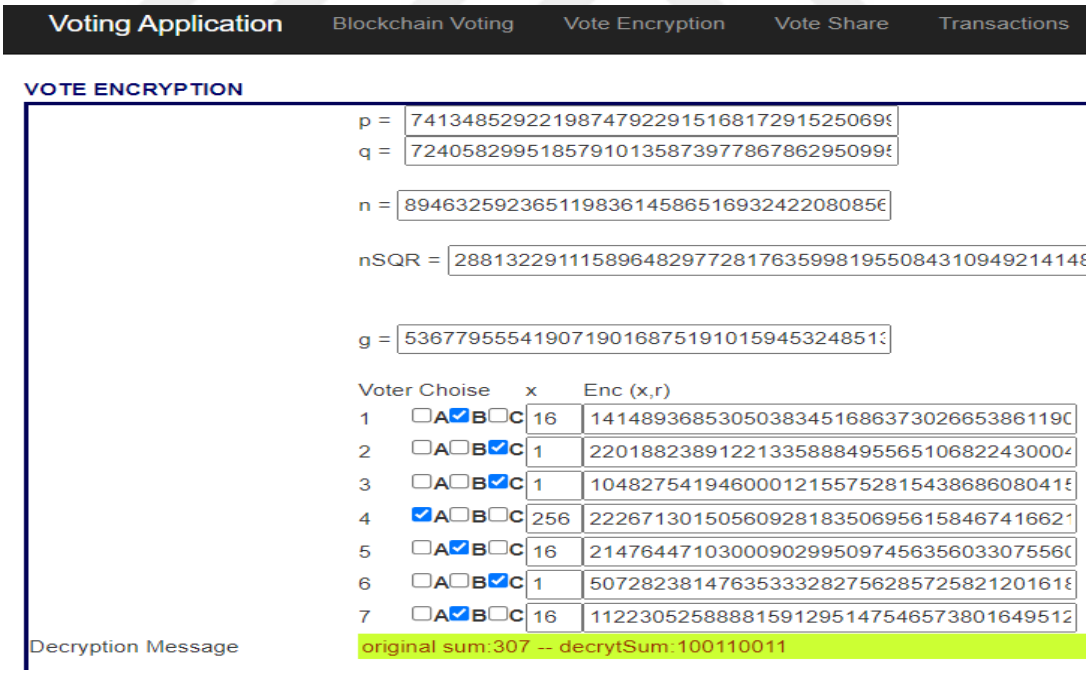
Şifre Çözme işlemi;

$$x = Dec(y) = \frac{L1}{L2} mod\ n = \frac{L\left(y^{\lambda}\ mod\ n^2\right)}{L(g^{\lambda}\ mod\ n^2)} mod\ n \tag{5.17}$$

Şekil 5.8'de Oylamaların yapıldığı uygulama simülasyon çıktısında ki örnek çıktılar gösterilmiştir. Uygulama testlerinde her kullanıcı için homomorfik şifreleme sürelerinin gösterildiği çizelge 5.6 incelenmiş, hesaplamanın ortalama 93 ms'de bittiği tespit edilmiştir.

Çizelge 5.6 Homomorfik şifreleme süreleri

Seçmen	Şifreleme Süresi (ms)
1	94
2	89
3	91
4	87
5	90
6	93
7	107



Şekil 5.8 Oylama şifreleme simülasyonu örnek çıktısı

Şifresi çözülen değerin ikilik sayıya dönüştürülmesinden sonra, her aday için sayım sonucu hesaplanabilmektedir.

$$ConvertToBinary\ (x) = (CountA)\ (CountB)\ (CountC) \quad (5.18)$$

Şekil 5.8'deki 307 değeri, ConvertToBinary (307) = (1) (0011) (0011) tam sayısal çevrimi sonrasında, adayların aldığı oyların toplamı A=1, B=3, C=3 olarak elde edilmektedir.

Kullanılan oyların anonimliği ve gizliliği homomorfik şifreleme ile sağlanmaktadır. Bununla birlikte, kullanılan oylar şifreli olarak saklansa da, veriyi blok zincirinde depolayan düğümlerde görülebilme olasılığı vardır. Bu nedenle şifrelenmiş oyları doğrudan düğümlere göndermek yerine, önce veriler parçalanmıştır ve farklı düğümlere gönderilerek saklanması önerilmiştir. Sayım sırasında ise belirli sayıda düğümün bir araya gelerek yeniden şifreli verilerin elde edilmesi sağlanmıştır. Bu şekilde oluşturulan yapı sayesinde veri bütünlüğünün belirli kriterler ile farklı düğümler yardımıyla da teyit edilebilmesi sağlanmıştır. Verilerin parçalanması ve parçalı verilerden tekrar orijinal verinin elde edilmesi simülasyonu için kullanılan sayfaya Google Drive linkinde yer alan "CloudTestApplication_TRTVotingWeb.rar" dosyası içindeki "Shamir.aspx" sayfasından erişebilirsiniz.

Veri parçalama algoritması şekil 5.9'da gösterilmiştir.

- Oy verileri 4 düğümde parçalandığında, P (p1,p2,p3,p4) (Şekil 5.5) şeklinde hesaplanabilmektedir.
- Tasarımda karar verilen en az düğüm sayısı bir araya gelerek veri bütünlüğünü sağlayabilmektedir. Örneğin en az 3 düğümün bir araya gelmesi istenildiğinde P = decryption (p1,p2,p4)

En az aynı sayıda farklı düğüm bir araya gelerek farklı bir doğrulama işlemini yapabilmektedir. P = decryption (p2,p3,p4)

	N düğüm, P Rastgele Asal Sayı
Girdi:	Gizli veri $a_0 = S$
Çıktı:	Shared data $(x_i, y_i)\ i = 0..N-1$
1	$(a_i)_{i=1....N-1}$ N − nd () // katsayıların hesaplanması
2	**for** *i* = 0 **to** *N* **do** // fonksiyon hesaplaması
3	$f(x) \leftarrow a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1}$
4	**for** *j* = 0 **to** *N* **do** // parçaları hesaplama
5	$y_j \leftarrow f(j) \bmod P$
6	**return** $(x_i, y_i)i$=0..*N*-1

Şekil 5.9 Veri parçalama algoritması

Örneğin; $p =$ rastgele asal sayı, a_1 ve a_2 rastgele sayılar, $S =$ gizli veri olarak gösterildiğinde fonksiyon aşağıdaki şeklide elde edilebilmektedir.

$$p \in \mathbb{P} : p > S, \quad p > n \tag{5.19}$$

$$a_i < p, a_0 = S \tag{5.20}$$

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} \tag{5.21}$$

$$a_0 = S \tag{5.22}$$

5 düğümlü sistemde, eşik değeri 3 düğüm olan bir sistemde.

$$f(x) = a_0 + a_1x + a_2x^2 \tag{5.23}$$

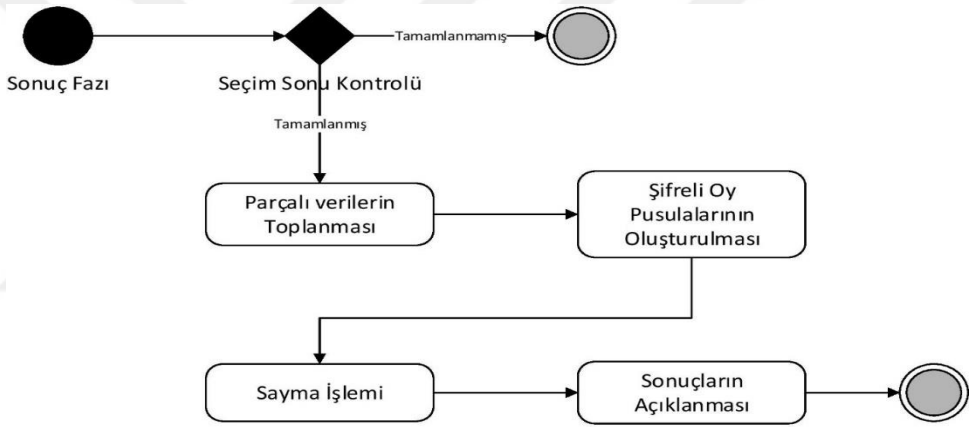
Verinin parçalara ayrılması sürecinde 5 düğüm için veriler 5 parçaya bölünmüştür. Bu veri parçalama işlemi, tüm düğüm sayısına göre dağıtılır ve rastgele düğümleri birleştirerek bunları oluşturmak ve kontrol etmek için çapraz kontrol sağlanabilmiştir.

$$D_0 = (1, f(1)\ mod\ p) = (1, y_0) \tag{5.24}$$

$$D_1 = (2, f(2)\ mod\ p) = (2, y_1)$$
$$D_2 = (3, f(3)\ mod\ p) = (3, y_2)$$
$$D_3 = (4, f(4)\ mod\ p) = (4, y_4)$$
$$D_4 = (5, f(5)\ mod\ p) = (5, y_5)$$

Orijinal veriler ve kontrol için rastgele seçilen en az 3 düğümle elde edilebilmektedir (Şekil 5.5, Şekil 5.10).

$$(x_0, y_0) = (1, y_0)$$
$$(x_1, y_1) = (2, y_1)$$
$$(x_2, y_2) = (4, y_2) \quad (5.25)$$



Şekil 5.10 Oy sayma fazı iş akış diyagramı

$$f(x) = \sum_{j=0}^{2} y_j . l_j\ (x) \quad (5.26)$$

$$l_j(x) := \prod_{0 \le m \le k} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \dots . \frac{(x - x_k)}{(x_j - x_k)} \quad (5.27)$$

$$m \neq j$$
$$k = 3\ (0,1,2)\ \ j = 0 \quad m \neq 0$$
$$l_0\ (x) = \frac{(x - x_1)}{(x_0 - x_1)} \frac{(x - x_2)}{(x_0 - x_2)} \quad (5.28)$$

$$k = 3\ (0,1,2)\ \ j = 1 \quad m \neq 1$$
$$l_1\ (x) = \frac{(x - x_0)}{(x_1 - x_0)} \frac{(x - x_2)}{(x_1 - x_2)} \tag{5.29}$$

$$k = 3\ (0,1,2)\ \ j = 2 \quad m \neq 2$$
$$l_2\ (x) = \frac{(x - x_0)}{(x_2 - x_0)} \frac{(x - x_1)}{(x_2 - x_1)} \tag{5.30}$$

$$f(x) = \sum_{j=0}^{2} y_j . l_j\ (x) \tag{5.31}$$

Her düğümden parçalanmış değerler kullanılarak fonksiyon elde edilmektedir.

$$f(x) = y_0 . l_0(x) + y_1 . l_1(x) + y_2 . l_2\ (x) \tag{5.32}$$

N Düğümler, P Asal Sayı

Girdi: $(x_i, y_i) i=0..N-1$

Çıktı: Gizli Veri S

1 **for j**= 0 **to k do** // kat sayıların oluşturulması

2 $l_j(x) \leftarrow \frac{(x-x_0)}{(x_j-x_0)} \ldots . \frac{(x-x_k)}{(x_j-x_k)}, k \neq j$

3 **for j**= 0 **to** *N* **do** // fonksiyonun oluşturulması

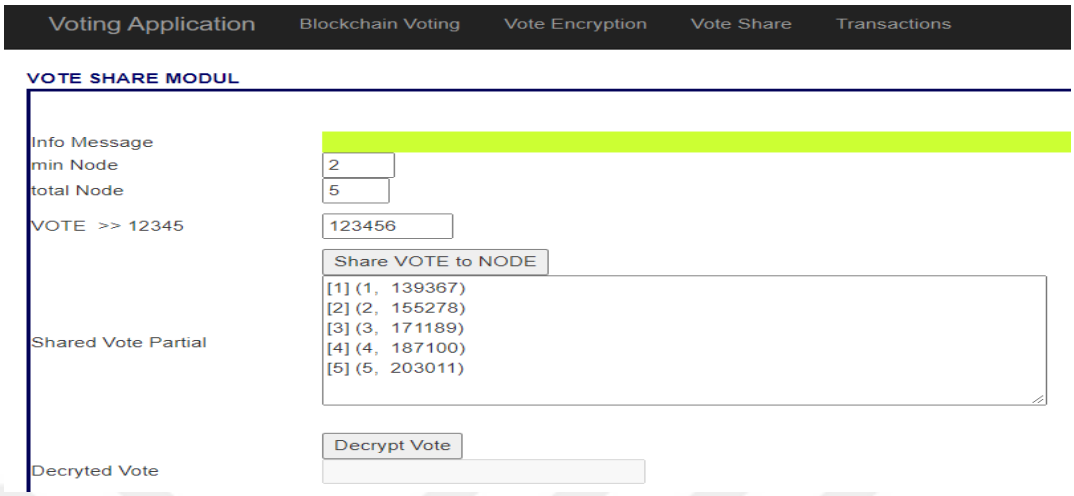
4 $f \leftarrow y_0 . l_0(x) + y_1 . l_1(x) .. y_{j-1} . l_{j-1}\ (x)$

5 $S \leftarrow f$ mod P// şifreli verinin oluşturulması

6 **return** S

Şekil 5.11 Yeniden veri oluşturma algoritması

Verilerin yeniden oluşturulması algoritması şekil 5.11'de gösterilmiştir. Uygulama çıktısı olarak elde edilen verilerin parçalanmış değerleri şekil 5.12'de gösterilmiştir.



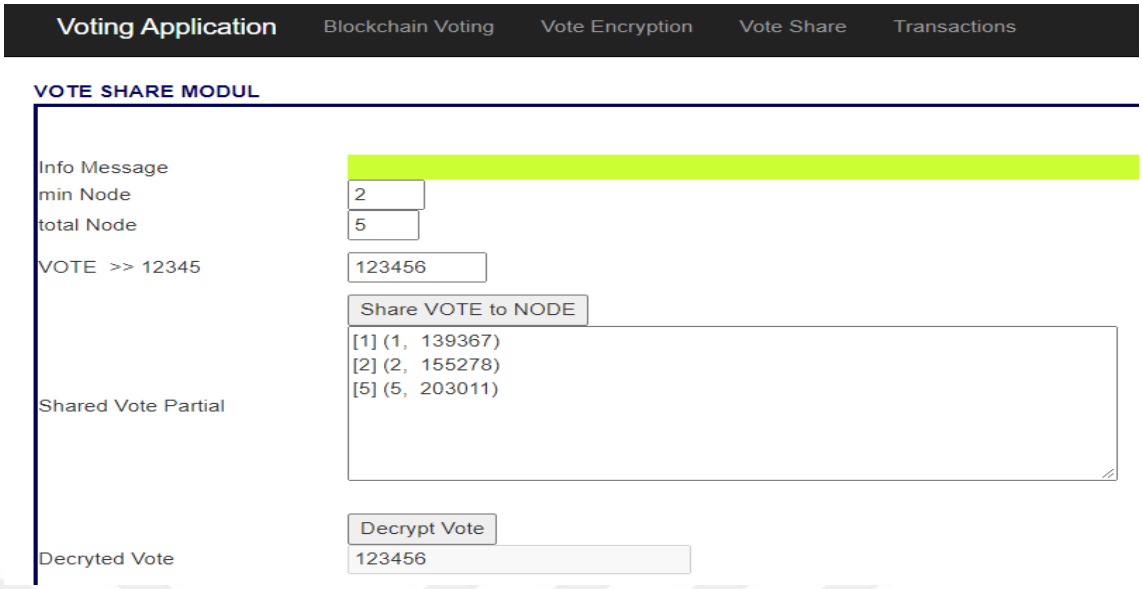
Şekil 5.12 Veri paylaşımı ekran görüntüsü

Son olarak mod p hesaplanarak gizli veri elde edilmektedir. Şekil 5.13'te 1, 2 ve 5 düğümleri seçilmiş ve orijinal veri elde edildiği gösterilmiştir.

$$f(x) = a_2x^2 + a_1x + a_0 \ (mod\ p) \tag{5.33}$$

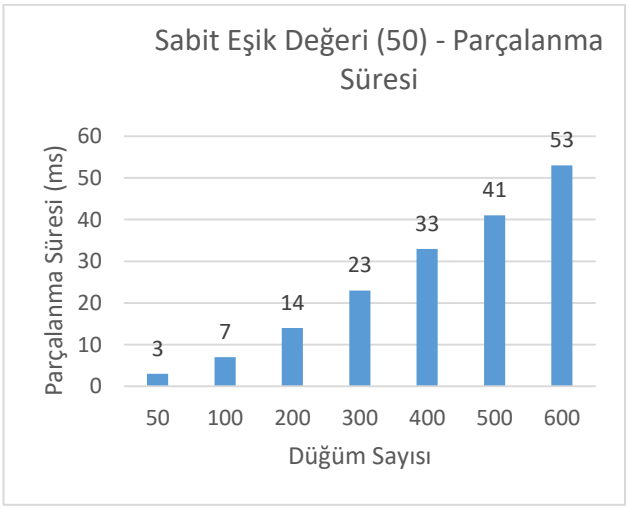
Gizli veri $S = a_0$ elde edilebilmektedir. Şekil 5.13 'te uygulama simülasyonunda 5 düğümden 3 tanesi seçilerek elde edilen veri gösterilmektedir.

Düğümler veya gözlemciler, tüm işlemlerin geçerliliğini kontrol ederek seçimin bir bütün olarak güvenli olduğundan ve verilerin tutarlı bir şekilde saklandığından emin olabilmektedir. Önerilen sistemde dağıtık ve karmaşık veri paylaşımı ile saldırganın verilere tek başına herhangi bir veriye erişmesi durumunda dahi, anlamlı verilere ulaşmasına izin vermemektedir.



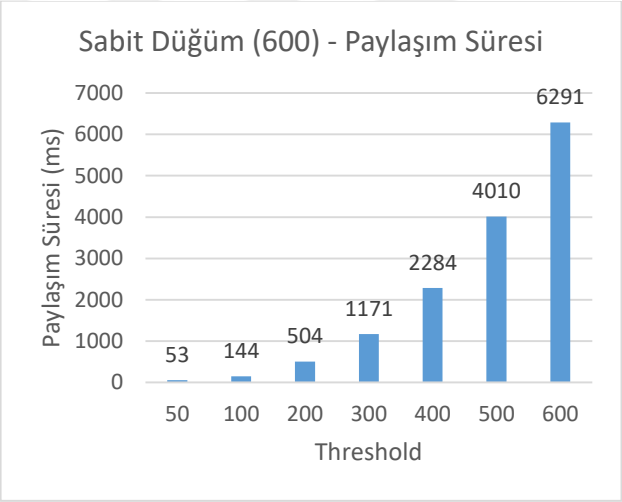
Şekil 5.13 Verilerin tekrar oluşturma ekran görüntüsü

Parçalı paylaşım için sabit eşikli (Şekil 5.14) ve sabit düğümlü (Şekil 5.15) hesaplama süreleri hesaplanmıştır. Eşik (threshold), parçalanmış düğümlerde depolanan değerin yeniden elde edileceği zaman bir araya gelmesi gereken minimum düğüm sayısını ifade etmektedir. Eşik sabit kaldığında düğüm sayısındaki artışın hesaplama süresinde artışa neden olduğu ancak değişimin doğrusal olduğu tespit edilmiştir. Ancak düğüm sayısı sabitlendiğinde ve eşik değeri artırıldığında hesaplama süresinde önemli artışlar olduğu tespit edilmiştir.



Şekil 5.14 Sabit eşik değeri (50) parçalanma süresi

İşlem sürelerinin gerçek sistem tasarımında optimum düğüm ve eşiklerin kullanılmasının oylama işlem süresini önemli ölçüde azaltacağını göstermektedir. Eşik değeri artırıldığında oy verme süresinin logaritmik olarak arttığı ve bunun seçim zamanını olumsuz etkilediği görülmüştür. Ayrıca eşik sayısının düşük bir değer seçilmesi durumunda da tekrar manipülasyona neden olma olasılığı ortaya çıkmaktadır. Yedeklilik, güvenlik ve verimlilik göz önüne alındığında 600 düğüm ve 300 eşik değerinin kabul edilebilir düzeyde olduğu değerlendirilmiştir. Seçilen değerler sistemin tasarımına göre kolayca azaltılıp artırılabilmektedir. 600 düğümde, 300 eşik değeri seçildiğinde, bir oyun sadece toplam süresi yaklaşık olarak 1,17 sn (7000 ms, şifreleme + paylaşım + işlem = 93 + 1171 + 5774) hesaplanmıştır (Şekil 5.15). Bununla birlikte, 150 milyondan fazla seçmenin oy kullandığı 3 Kasım 2020'de yapılan son ABD başkanlık seçimleri gibi büyük bir seçmen listesinin olduğu bir seçim organizasyonunda daha fazla düğüm ihtiyacının olması beklenmektedir. (Anonymous 2020c).



Şekil 5.15 Sabit düğüm (600) paylaşım süresi

E-oylamada ortaya çıkabilecek problemleri çözmek içinde ayrıca, klasik oylamada olduğu gibi bölgelerde seçim çıktılarının da saklanması ile hibrid bir yapı oluşturularak daha da sıkılaştırma yapılabilir. Bizim önerimizde parmak izli kimlik kartı kullanımı, homomorfik şifreleme ve verilerin dağıtılmış yapısı birleştirilerek oylama sisteminin güvenliği sağlanmaktadır. Bu yöntem herhangi bir özel blok zinciri sistemine entegre edilerek, seçim sırasında özellikle sonuç sızıntılarının meydana gelmesi, başkası adına oy

kullanılması, birden fazla oy kullanılması ve sayım işlemlerinde ortaya çıkan manipülasyonların engellenmesi sağlanabilmektedir.

5.3 Sistemin Güvenlik Analizi

a) Sadece kayıtlı seçmenler oylarını kullanmalıdır.

Öncelikle tüm seçmen listesi otorite tarafından hazırlanmaktadır. Daha sonra seçmenlerin seçim öncesinde kayıt yaptırması gerekmektedir. Kayıt sırasında önceden alınmış biyometrik kimlik kartı doğrulaması yapılarak kayıt güncellemesi sağlanmalıdır. Önerilen sistemde başarılı bir şekilde kayıt kontrol sürecini tamamlamış olan seçmenlere (v_i) token dağıtımı yapılarak ve şifre belirlenmesi sağlanmıştır. Örnek uygulamamızda token kişinin mail adresine link olarak gönderilmiştir. Tokenların pusula olarak verilmesi kişi token ilişkinin kurulmaması için önemlidir. Bu şekilde sadece token sahibi biyometrik veri kontrolü ile kabul edilen seçmenlerin oy kullanmasına izin verileceğinden, sadece oy kullanma yetkisi bulunanların oy kullanması sağlanması hedeflenmiştir. Her seçmenin kimlik kartı ve oy kullanmada kullanacağı hesap bilgisi olmalıdır. v_n seçmenleri göstermektedir.

$$\exists v_n \forall\, token_n (P(token_n) \leftrightarrow\ token_n =\ v_n \tag{5.34}$$

Şüpheli kayıtlı olmayan ve elinde geçerli token bulunmayan seçmenin seçim günü doğrulama süreçlerini tamamlanmasına izin verilmeyeceği gibi, biyometrik eşleştirmede olmayacağından başka birinin yerine oy kullanması da engellenmiş olacaktır. Ayrıca sistemde kayıtlı seçmen listesi oluşturularak, kimlerin oy kullandığıda bağımsız olarak takip edebilecektir.

b) Her seçmen sadece bir kez oy kullanabilmelidir.

Önerilen sistemde her seçmen oy verme sırasında seçmen listesinde oy kullandı olarak işaretlenmiştir. Başka bir token ile oy vermesi engellenerek, ayrıca kullanılan token akıllı sözleşmelerde de işaretlenerek aynı tokenla yeni bir oy verme işlemide engellenmiştir. Akıllı sözleşmelerle mükerrer oy kullanımlarını da tespit ederek engellenmiştir. Tüm veri tabanının içeriği aşağıdaki gibi görünmelidir,

$$v_n\ \rightarrow Oy\ Kullandı = true \tag{5.35}$$

Akıllı sözleşme içinde de token kontrolü sonrasında,

mapping (address => bool) public voted; (5.36)

Geliştirilen sistemde aynı seçmenin tekrar aynı token için yeni bir tercih göndermek istemesi durumunda, token doğrulaması sırasında kullanılmış olarak gözükeceği için yeniden oy göndermesine izin verilmemiştir. Sistem her seçmen için yalnızca ilk gönderimi saklayacak ve aynı token için gelen diğer gönderimleri kabul etmesi engellenecek şeklide tasarlanmıştır. Bu sayede her seçmenin yalnızca bir kez oy vermesine izin verilen ve ilk oyu verildikten sonra tekrar oy kullanmasına izin verilmeyen tüm normal seçimlerde benimsenen standart uygulama özellikleri sağlanmıştır.

c) Güvenilir olmalıdır, veriler değiştirilememelidir.

Bir blok zinciri veri tabanı, merkezi olmayan bir veri tabanıdır. Bu sistemde veri tabanını yöneten merkezi bir sunucu olmadığı, ancak herkesin tüm veri tabanının en son sürümüne sahip olduğu bir yapıdır. İlk olarak, her blok önceki bloğun blok başlığının özet değerini içererek büyümektedir. Bu durum yeni bloklar eklenirken hiçbir şeyin değiştirilmemesini sağlamaktadır. Her hangi bir değişiklikte zincir bozulacağından diğer madenciler tarafından kabul edilmeyecektir. Özet fonksiyonuna tabi olan değerde tek harf değişikliğinde bile çok farklı değerler ortaya çıkmaktadır. Buda zincir yapısını değiştireceğinden kabul edilmez bir durum tespit edilmiş olacaktır.

Önerilen sistemde Ethereum blok zinciri altyapısı kullanılarak verilerin zincir yapısında değiştirilemez özeliklerde saklanmaları sağlanmıştır. Bu zincir yapıları kayıtların bütünlüğünü korumak için Merkle ağacı kullanmaktadır. Öncelikle her bir işlemin özet değerleri alınarak çalışmaktadır. Karma çiftleri daha sonra tek bir kök karma değeri ile sonuçlanana kadar birleştirilmektedir. İşlemler bu yapı ile kolayca doğrulanabilmektedir.

d) Her veri anonim olarak kaydedilmelidir.

Seçmenin kimliği ile token bağlantısı olmadığı gibi, kullanılan oylarda tamamen dağıtık ve şifreli olduğundan, sistemde tercih ve kimlik ilişkisi kurulamayacağı anlamına gelmektedir. Önerilen sistemde homomorfik şifreleme sırasında olasılıklı bir şifreleme yöntemini kullanılmıştır. Bu sayede aynı tercih değeri birden çok kez şifrelense bile, şifrelenmiş verilerde her zaman farklı bir değer elde edilerek anonimlik sağlanmıştır.

Kullanılan şifreleme algoritması x mesajına karşılık her seferinde rastgele bir r değeri kullanmaktadır.

$$\text{HomomorfikSifreleme}(x, r) = g^x . r^n mod\ n^2 \tag{5.37}$$

$$m_n \in M, M\ Seçenekler \tag{5.38}$$

$$\text{HomomorfikSifreleme}(m_n, r1) \neq \text{HomomorfikSifreleme}\ (m_n, r2)$$

Ayrıca, şifreli değerlerin çözümlenmeden, şifreli veriler üzerinden sayım işlemleri gerçekleştirildiği için anonimlik korunmuştur. Bu işleri gerçekleştirebilmek için homomorfik şifreleme tekniğinin toplama özelliği kullanılmıştır.

$$C_1 = \text{HomomorfikSifreleme}\ (m_1, \text{r})\ \ C_2 = \text{HomomorfikSifreleme}\ (m_2, \text{r}) \tag{5.39}$$

$$m_1 + m_2 = \text{ŞifreÇözme}\ (C_1, C_2)$$

e) Tüm oyların düzgün sayıldığı doğrulanabilmelidir.

Önerilen sistemde, resmi olarak yayınlanan sonuçları kontrol için farklı düğümler bir araya gelerek sonucu yeniden hesaplayarak doğrulayabilmektedir. Seçmen tarafından yapılan tercih önce şifrelenmiştir, daha sonra şifreli içerik, sonucun farklı kombinasyonlarla doğrulanabilmesi için parçalanarak diğer düğümlerde saklanması sağlanmıştır. Tasarlanan yapıda doğru sonucu elde edebilmek için, en az sayıda düğümün bir araya gelerek doğrulama işlemini yapmaları zorunlu tutulmuştur. Ayrıca bu özellik sayesinde saklanan verilerin çapraz doğrulanabilmesi sayesinde verilerin yedekliliği de sağlanmıştır.

Aşağıdaki örnekte 3 adet düğümün bir araya gelerek gizli veriyi elde ederek doğrulama yapabilmesini sağlayan fonksiyon örneği sunulmuştur. Bu özellik sistem tanımlaması bölümünde detaylı olarak incelenmiştir (Şekil 5.5, Şekil 5.10).

$$Gizli\ veri = a_0$$

$$f(x) = y_0 . l_0(x) + y_1 . l_1(x) + y_2 . l_2\ (x) \tag{5.40}$$

$$f(x) = a_2 x^2 + a_1 x + a_0\ \ (mod\ p)$$

f) Saldırılara karşı dayanıklı olmalıdır.

Hizmet Reddi (DDos) saldırısı; Kötü niyetli bir düğüm, blok zincirine geçerli bir işlemi eklemeyi kabul etmeyerek sistemi çalışmaz duruma getirebilir. Saldırganın başarılı olabilmesi için, ağdaki her düğüm için DDoS yapması gerekmektedir. Dağıtık yapıda fazla sayıda düğüm olacağından diğer düğümler geçerli işlemin kayıt işlemini tamamlayacağından işlemlerin kesintisiz devam etmesi sağlanmaktadır. Tasarlanan sistemde iki düğümlü bir yapı oluşturulmuştur. Her iki düğümde de verilerin güncel olarak hizmet vermeye devam etmeleri sağlanmıştır. Ayrıca, dağıtık özel izinli düğümlerden oluşan sisteme dışarıdan saldırı olmayacağı gibi, içerden olabilecek saldırılarda veya arızalarda diğer düğümler ayakta olacağından sistemler çalışmaya devam edecektir.

Sybil saldırısı; Sybil saldırısı ağ operasyonunu kesintiye uğratmak için büyük miktarda düğümün oluşturulduğu sistemler olarak bilinmektedir (Hjálmarsson vd. 2018). Swathi ve arkadaşlarının yaptıkları çalışmada, düğümlerin oluşturduğu verilerin incelenebileceği veya izinli sistemlerin Sybil saldırılarını önlemede yardımcı olacağı belirtilmiştir (Swathi vd. 2019). Düğümlerin ağa katılmadan önce kimliklerini kanıtlamaları gerekiyorsa, kimlik sahtekârlığı yapamayacaklardır (Singh vd. 2021). Önerdiğimiz sistemin de özel bir ağda çalıştırılması sebebiyle, izinsiz olarak yeni bir düğümün ve hesabın oluşturmasına izin verilmemektedir. Seçim öncesi kullanıcı tokenları, ip adresi sabitlenmiş düğümlerden seçmen sayısı kadar üretilmiştir. Daha sonra oluşturulan tokenlar akıllı sözleşmeye eklenerek, akıllı sözleşmelerin sisteme önceden yüklemeleri yapılmıştır. Yeni bir güncelleme ihtiyacında tüm sistemdeki yüklemelerin yeniden tüm düğümlerde yapılması gerekmiştir. Gerçek bir sistemde çok fazla düğüm olacağından bu tür bir saldırı için gerekli ortam sağlanamayacaktır.

Ortadaki Adam Saldırısı (Man in the Middle Attack-MITM); Ortadaki adam saldırısında saldırgan iletişimi kendisinin istediği şekilde yönlendirebilmesi olarak tanımlanmaktadır. Genellikle network katmanında ağ anahtarlarına eklenen yeni bir cihaz üzerine veya kablosuz ağa eklenen yeni bir AP (Access Point) kurulması ile bu yönlendirmeler yapılabilmektedir (Ortega vd. 2009). Ortadaki adam saldırıları, meşru bir kullanıcıdan gelen trafiği değiştirmek için ARP (Address Resolution Protocol) sahtekârlığını (ARP poisoning / ARP spoofing) kullanılmaktadır. LAN üzerindeki cihazlar IP adresi üzerinden iletişim kurmaz bunun yerine ARP kullanılmaktadır. ARP

tabloları, IP adresini bir MAC adresine çevirmekte kullanılmaktadır. Saldırgan MAC tablosunu değiştirmeye çalışarak bu işlemi yapabilmektedir. Saldırganın araya girerek kullanıcı ve uygulama arasındaki iletişimi dinleyerek kendi üzerinden geçirebildiği takdirde trafiği anlamlandırması mümkün olabilmektedir. Önerilen sistemde, kablosuz ağ veya açık internet sistemlerinin kullanılmasına izin verilmemektedir. Sistemlerde kullanılan IP ve MAC tablosu sabitlenerek yeni IP dağıtımının dağıtılması engellenmiştir. Ayrıca, tüm sistemdeki verilerin SSL bağlantılı VPN networkler üzerinden haberleşmesi sağlanarak açık veri transferine izin verilmemiştir.

Önerilen sistemde kullanılan oylar öncelikle homomorfik şifre ile anonimleştirilmektedir. Uygulanan şifreleme yöntemi neticesinde aynı tercih sonucunda da eşit olmayan değerler elde edilmektedir. Bu sebeple oy pusulalarının içeriğinin ayırt edilmesi engellenmiştir.

$$\text{HomomorfikSifreleme}(m_n, r1) \neq \text{HomomorfikSifreleme}\ (m_n, r2) \quad (5.41)$$

Daha sonrasında, sistem üzerinde düğümlere gönderilen veriler için 34 basamaklı bir asal sayı kullanılmıştır. Bu uzunluktaki bir şifrenin tahmin edilmesi oldukça zordur. Bu şifrenin tespit edilmesi durumunda da tüm düğümlere (600 düğüm veya üzeri) gönderilen değerlerin yakalanarak değiştirilmesi gerekmektedir. Bu durumda saldırganın o seçim istasyonundan gelen tüm trafiği iptal edip tamamen baştan oluşturduğu verilerle değiştirmesi gerekmektedir. Ayrıca, önerilen mimaride gönderilen mesajlar SSL sertifika kullanılarak yapıldığından bu içeriklerin çözümlenmesini ve özel anahtar ile imzalanıp gönderilmesi de saldırıyı daha da zorlaştırmaktadır. (Angin 2020). Ayrıca kullanılan oy bastırılarak saklanması neticesinde de oyların çapraz sayılmasıyla da ek kontrol noktalarının oluşturulması mümkündür.

% 51 saldırısı; Blok zincirine özel bir saldırı türü olarak karşımıza çıkan bu saldırıda, saldırganın amacı, işlem gücünün% 51'ine sahip olarak sistemi kontrol etmek istemesi olarak ortaya çıkmaktadır (Singh vd. 2021). Bu duruma düşmemek için, sisteme dâhil olan kaynaklar izinli olarak eklemeleri yapılmıştır. Ayrıca doğrulama sayısının artırılmasıda saldırıyı önlemek için uygulanmalıdır Art niyetli saldırganların sisteme kendilerini eklemeleri mümkün değildir. Ayrıca bu saldırı için tasarlanan büyük bir sistemdeki kaynak ihtiyacı bu tür bir saldırı karşısında da engelleyici durumundadır.

Eklemenin yapılabilmesi için sistemlerin aynı konfigürasyonla ve aynı genesis.blok yapısında kurulmuş olması diğer düğümlere erişebiliyor olması gerekmektedir (Anonymous 2021.). Daha önce başlatılan düğüme bağlamak istenildiğinde, bunu konsoldan bir eş olarak aşağıda kod yardımıyla eklemek gerekmektedir. Bu işlemin tüm sistemdeki diğer düğümler de yapılması gerekeceğinden bu tür bir işleme izin verilmemiştir. Klasik Ethereum kurulumlarında da benzer yöntemlerle yetkili düğümler kontrollü ve yetkili kişilerce yapılmalıdır.

Sistem içinde rol alan birimlerin ortaya çıkarabileceği risk durumları açısından ayrı bir değerlendirme yapıldığında,

Seçmenin yapabileceği saldırılar: Çoklu oy kullanma, bu durum oluşmaması için hem veri tabanı kısmında hem de akıllı sözleşme tarafında gerekli kontroller yapılarak engellenmektedir. *Başkasının yerine oy kullanma veya oy satın alma*, seçmenler biyometrik bilgi kontrolü yapılarak oy verme işlemi yapabilecekleri için bu duruma izin verilmemektedir. Ancak tüm internete açık uzaktan oy verme durumlarında bu durumun oluşabileceği değerlendirilmiştir.

Sistem yöneticisi ve otorite bileşenlerinin yapabileceği saldırılar: Seçmen listesinde fazla seçmen oluşturulması söz konusu olabilir. Tekil kullanıcı kayıt işlemini sağlayacak ek kontrollerin yapılması gerekmektedir. Kayıt olmayanlar için token oluşturma; kayıt zamanı dışında token oluşturmaya izin verilmemektedir. Seçim sonuçlarının yanlış açıklanması; seçim verilerinin blok zinciri üzerinde tutulması sebebiyle değiştirilmesine izin verilmemektedir. Ayrıca, tasarlanan sistemde otorite haricinde çapraz sorgularla sayım sonuçlarının kontrol edilmesi sağlanmıştır.

Madencilerin yapabileceği saldırılar: Madenciler sistemde bazı işlemleri kayıt etmeyebilirler. Bu durumu önlemek için dengeli bir şekilde farklı parti ve kişilerden oluşan mümkün olduğunca kalabalık bir madenci yapısı oluşturulması öngörülmüştür. Önerilen sistemin faydaları ise aşağıdaki şekilde ifade edilebilir.

- Yüksek kullanılabilirlik; sistem eşler arası bir ağdaki yüzlerce düğüme dayandığından ve veriler her bir düğümde çoğaltılıp güncellendiğinden, sistem yüksek oranda kullanılabilir hale gelmektedir. Düğümlerde oluşabilecek olası

problemlerde de sistem bir bütün olarak çalıştığından çalışmaya devam ederek, yüksek oranda erişilebilirlik devam etmektedir.

- Tek Merkeziyet özelliğinin olmaması; blok zincirinin temel bir kavramı ve faydasıdır. İşlemleri doğrulamak için güvenilir bir üçüncü şahsa veya aracıya gerek yoktur; bunun yerine işlemlerin geçerliliğini kabul etmek için bir fikir birliği mekanizması kullanılmaktadır.
- Değişmezlik; veriler blok zincirine yazıldıktan sonra verilerin değiştirilemeyecek olması seçmenler üzerinde güven ortamı oluşturacaktır. Özetleme (hashing) blok zincirinden veri bütünlüğünün sağlanmasında yardımcı olmaktadır.
- Kullanılan oy ve seçmen ilişkisi olmadan oy kullanabilme ve sayım işlemlerinin tamamlanması mümkün olmaktadır. Sayım işlemlerinin bağımsız paydaşlar tarafından da doğrulanması mümkündür.

6. SONUÇLAR

Elektronik oylama uzun yıllardır ilgi konusu olmasına rağmen, hala tam olarak çözülemediği ve yaygın olarak kabul görmediği görülmektedir. Sayısız elektronik sistem önerisi sunulmuştur ve kullanılmıştır. Ancak bu sistemler içerisinde tespit edilen güvenlik açıkları nedeniyle seçimlerin bütünlüğü ile ilgili bazı şüpheler ortadan kalkmamıştır. Sisteme olan güven problemi olarak öne çıkan sebepler neticesinde sürekli şüphe ile yaklaşılmıştır. Çevrimiçi oylamadaki merkeziyetçi anlayışın, sistemlerde tespit edilmesi zor oy sahtekârlığına veya manipülasyonlara sebep olabileceği ihtimali her zaman tartışılmaya devam etmektedir.

Bu tez çalışması kapsamında, seçmenin bu konulardaki güvenini sağlamaya yönelik olarak blok zinciri alt yapısının avantajlarını kullanan, seçimler sırasında veya seçim sonuçlarının açıklanması sırasında ortaya çıkabilecek manipülasyonları önlemek amacıyla çift katmanlı bir güvenlik modeli önerilmiş, şifreleme özellikleri geliştirilmiş ve test edilmiştir. Simülasyon neticesinde, önerilen sistemin oylama ve sayma aşamalarının amaçlandığı gibi çalıştığı tespit edilmiştir. Oylar öncelikli olarak homomorfik şifrelemenin homomorfik toplama özelliği sayesinde şifreli metinler üzerinden işlemlere tabi tutularak gerekli anonimlik sağlanmıştır. Şifrelenmiş verilerin parçalanarak dağıtılması yardımıyla da çapraz doğrulama imkânı eklenmiştir. Yalnızca kayıtlı seçmenin, bir kez oy vermesini sağlayan akıllı sözleşme kullanımı özeliğinin de eklenmesi ile çoklu oy kullanımı ihtimali ortadan kaldırılmıştır. Blok zinciri altyapısını tamamen açık tasarlanması, uygulamanın da tüm internete açılması durumunda da kullanılabileceği değerlendirilmiştir. Ancak bu tür bir sistemde kontrol edilmeyen bazı bileşenler bulunmaktadır. Örneğin seçmenin cihaz güvenliğini sağlanmanın zorluğu, oy satın alma ihtimalinin varlığı gibi unsurlar hala risk oluşturmaya devam etmektedir.

Önerilen sistemde, sistemin dağıtık mimarı tasarımı ve kurulumu neticesinde, bir düğümün çalışamaz duruma geldiğinde de sistemin kesintisiz olarak çalışmaya devam etmesi sağlanmıştır. Sistemin kesintisizliği veri kaybı olmadan çalıştığı tespit edilmiştir. Seçim sonuçlarının hesaplanması ve açıklanmasına yönelik farklı düğümlerin oluşturduğu doğrulama neticesinde de manipülasyonlara izin vermeyen bir ortam oluşması sağlanmıştır.

Sistemin sonuçlarını analiz ederken karşılaşılan zorluklar ise, gerçek bir seçim sisteminin ihtiyaç duyduğu kadar çok düğümlü simülasyon ortamının oluşturmanın zorluğu olmuştur. Ayrıca sisteme güvenlik önlemleri için eklenen çift katmanlı şifreleme işlemlerinin ek zaman maliyeti oluşturduğu görülmüştür. Gelecekte daha gerçekçi bir sistemle simule edilmesi, sistemin uçtan uca her aşamasının çalıştırılması ve sistemin ölçeklenebilirliği için optimizasyonlara odaklanılması hedeflenmektedir.

6.1 Sınırlamalar ve Gelecek Çalışmalar

Özellikle elektronik sistemlerle desteklenen oylama sistemleri her zaman tüm dünyada ilgi odağı olmaya devam etmektedir. Elektronik sistemlerin seçim sistemlerine katkı sağlayacağı bilinmektedir. Blok zinciri teknolojisinin de bu kapsamda değerlendirilmesi önemlidir. Ancak, diğer uygulanan sistemlerden farklı sistem mimarisine, uygulama geliştirme özeliklerine sahip olması nedeniyle potansiyel farklı güvenlik açıklıklarını barındırabildiği de görülmüştür. Bu sebeple, e-oylama yöntemine geçiş için, önce küçük pilot popülasyonlarda uygulanıp ardından kapsamı yavaşça genişleterek ilerlenmesi gerektiği ortak kanaat olarak kabul görmektedir. Sonuç olarak; özellikle yeni ortaya çıkan sistemlerin de kendi riskleriyle birlikte geldikleri değerlendirilerek, bu tür oylama sistemlerinin uygulanması sırasında geliştiriciler ve hükümetler için hala birçok zorluk ve risk oluşturabileceği göz ardı edilmemelidir. Ancak mevcut bazı güvenlik risklerinin ortadan kalkmasına yardım edecek bir ortamı tesis etmek için de yeni teknolojilerin sunduğu imkânlarında değerlendirilmesi önemlidir.

Bu kapsamda sınırlılıklar ve gelecekte yapılabilecekler aşağıdakiler gibi sıralanabilir.

- Bulut ortamlarının yaygınlaşmasının sistem tasarımlarında ek bazı özellikler ve esneklikler kazandırabileceği değerlendirilmelidir. Ancak bu tür durumlarda sistemlerin önceden iyi planlanması gerekmektedir, Örneğin, bizim bu tezde simulasyon için kullandığımız bulut hizmeti sonlandırılmıştır.
- Blok zincirindeki şifreleme ve işlemlerin doğrulanması süreçlerinin hız problemlerinin iyileştirilmesinin, süreçleri hızlandırabileceği değerlendirilmektedir.

- İnternete açık sistemlerdeki özellikle son kullanıcılardaki yazılım ve donanım güvenliğinin sağlanamaması sebebiyle zafiyetlerin oluşabileceği bu sebeple bu sistemler için çözümlerin sunulmasının önemli olduğu değerlendirilmiştir.
- Blok zinciri sistemleri gelişmekte olan yapılardır. Geliştiriciler tarafından bile bilinmeyen bazı açıklıklar barındırabilmektedir. Bu tür açıklıklar saldırgan tarafından önceden keşfedilip sıfırıncı gün saldırısı (Zero Day Attack) yapılabilmektedir. Bu tür saldırılara karşıda gerekli önlemlerin alınmasının faydalı olacağı değerlendirilmektedir.
- Blok zinciri tabanlı oylama sisteminin toplam işletme maliyetlerinin (enerji, geliştirme, uygulama vb.), klasik kağıt tabanlı oy sistemlerine göre uzun vade de avantajlı olabileceği değerlendirilmektedir. Ancak uygulamanın detaylı maliyet değerlendirilmesin yapılmasının uygulanabilirlik açısından faydalı olacağı değerlendirilmiştir.

KAYNAKLAR

Abdelwahab, A. 2017. An Introduction to Blockchain. Regional Forum on Cybersecurity in the Era of Emerging Technologies & the Second Meeting of the Successful Administrative Practices, 28-29 November, Cairo. Egypt.

Abuelhija, A., Abudouleh, A., Abumuhsen, B. ve Awad, F. 2020. Secure Voting System Using Distributed Ledger Technology. 2020 11th International Conference on Information and Communication Systems (ICICS), 7-9 April, 48-52, Irbid, Jordan.

Abuidris, Y., Hassan, A., Hadabi, A. ve Elfadul, I. 2019. Risks and Opportunities of Blockchain Based on E-Voting Systems. 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 14-15 December, 365-368, Chengdu, China.

Achieng, M. ve Ruhode, E. 2013. The adoption and challenges of electronic voting technologies within the South African context. International Journal of Managing Information Technology (IJMIT), November 2013, 5(4).

Adiputra, C. K., Hjort, R. ve Sato, H. 2018. A Proposal of Blockchain-Based Electronic Voting System. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 22-27, 30-31 October 2018; London, UK.

Agbesi, S. ve Asante, G. 2019. Electronic Voting Recording System Based on Blockchain Technology. 2019 12th CMI Conference on Cybersecurity and Privacy (CMI) , 28-29 November, 1-8, Copenhagen, Denmark.

Ajay, K. Bharath, B. M V Akhil, M. V. Akanksh, R ve Hemavathi, P. 2018. Intellectual Property Management Using Blockchain. 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 15-16 November, 428-430, Coimbatore, India.

Akbari, E., Wu, Q., Zhao, W., Arabnia, H. R. ve Yang, M. Q. 2017. From Blockchain to Internet-Based Voting. 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 11-14 July, 218-221, Las Vegas, NV, USA.

Alaya, B., Laouamer, L. ve Msilini, N. 2020. Homomorphic encryption systems statement: Trends and challenges. Computer Science Review, 36, 100235.

Alharby, M. ve van Moorsel, A. 2017. Blockchain-based Smart Contracts: A Systematic Mapping Study. Computer Science & Information Technology (CS & IT), 125-140.

Ali, S. T. ve Murray, J. 2016. An Overview of End-to-End Verifiable Voting Systems. Cryptography and Security, ArXiv:1605.08554.

Alkan, M. Ö. 2006. Türkiye'de Seçim Sistemi Tercihinin Misyon Boyutu ve Demokratik Gelişime Etkileri. Anayasa Yargısı. 23; 133-165.

Anane, R., Freeland, R. ve Theodoropoulos, G. 2007. E-Voting Requirements and Implementation. The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), 23-26 July, 382-392, Tokyo, Japan.

Andrian, H. R., Kurniawan, N. B., ve Suhardi. 2018. Blockchain Technology and Implementation: A Systematic Literature Review. 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 22-26 October, 370-374, Bandung - Padang, Indonesia.

Angin, P. 2020. Askeri Otonom Sistemlerde Blokzincir Tabanlı Veri Güvenliği. European Journal of Science and Technology. 362-368.

Anonim. 2020. Seçim Mevzuatı. Web Sitesi: http://www.ysk.gov.tr/. Erişim Tarihi: 19.12.2016.

Anonim. 2021. Seçimlerin Temel Hükümleri Ve Seçmen Kütükleri Hakkında Kanun. Web Adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=298&MevzuatTur=1&MevzuatTertip=4. Erişim Tarihi: 15.09.2021.

Anonymous. 2015. Virginia Information Technologies Agency. Web Sistesi: https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf. Erişim Tarihi: 03.04.2020.

Anonymous 2020a. Bitcoin. 2020. Web Sitesi: https://en.bitcoin.it/wiki/Main_Page. Erişim Tarihi: 13.04.2020.

Anonymous 2020b. Web Sitesi: https://www.coindesk.com/price/bitcoin. Erişim Tarihi: 13.04.2020.

Anonymous. 2020c. Web Sitesi: https://www.theguardian.com/us-news/ng-interactive/2020/dec/08/us-election-results-2020-joe-biden-defeats-donald-trump-to-win-presidency. Erişim Tarihi: 16.12.2020.

Anonymous. 2021. Private Network Tutorial | Go Ethereum. Web Sitesi: https://geth.ethereum.org/docs/getting-started/private-net, Erişim Tarihi: 31.07.2021.

Balasubramanian, K. ve Jayanthi, M. 2016. A Homomorphic Crypto System for Electronic Election Schemes. Circuits and Systems, 07(10); 3193-3203.

Bao, Z., Wang, B. ve Shi, W. 2018. A Privacy-Preserving, Decentralized and Functional Bitcoin E-Voting Protocol. 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart

City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 8-12 October, 252-256, Guangzhou, China.

Bartolucci, S., Bernat, P. ve Joseph, D. 2018. SHARVOT: Secret SHARe-based VOTing on the blockchain. Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, 27 May, 30-34, Gothenburg, Sweden.

Bashir, I. ve Safari, an O. M. C. 2017. Tiers of Blockchian Technology. Mastering Blockchain—Master the theoretical and technical foundations of Blockchain technology and explore future of Blockchain technology. Packt Publishing, 67-68, Birmingham, UK.

Bellare, M. ve Neven, G. 2006. Identity-Based Multi-signatures from RSA. Topics in Cryptology – CT-RSA 2007, Springer, 145-162, Berlin, Heidelberg, Germany.

Bellini, E., Ceravolo, P. ve Damiani, E. (2019). Blockchain-Based E-Vote-as-a-Service. 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 8-13 July, 484-486. Milan, Italy.

Bender, A., Katz, J. ve Morselli, R. 2005. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles. Web Sitesi: https://eprint.iacr.org/2005/304, Erişim Tarihi: 19.07.2020.

Benita K, R., Kumar S, G., B, M. ve A, M. 2020. Authentic Drug Usage and Tracking with Blockchain Using Mobile Apps. International Association of Online Engineering. LearnTechLib, 20-32, Waynesville, USA.

Bernhard, M., Benaloh, J., Alex Halderman, J., Rivest, R. L., Ryan, P. Y. A., Stark, P. B., Wallach, D. S. 2017. Public Evidence from Secret Ballots. Electronic Voting, Springer, 84-109, Berlin, Heidelberg, Germany.

Bilow, S. C. 2020. Introduction: Blockchain in Media and Entertainment. SMPTE Motion Imaging Journal. 129 (1); 20 – 21.

Bishop, M. ve Wagner, D. 2007. Risks of e-voting. Communications of the ACM, 50(11); 120.

Bishop, S. and Hoeffler, A. 2016. Free and fair elections: A new database. Journal Of Peace Research, 53 (4); 608-616.

Blanc, J. 2007. Electronic Voting. Challenging the Norms and Standards of Election Administration, IFES, 11-19, Virginia, USA.

Bokslag, W. ve de Vries, M. 2016. Evaluating e-voting: Theory and practice. Computer Science, ArXiv:1602.02509.

Boldyreva, A., Palacio, A. ve Warinschi, B. 2003. Secure Proxy Signature Schemes for Delegation of Signing Rights. Web Sitesi: https://eprint.iacr.org/2003/096. Erişim Tarihi: 18.07.2020

Bollinger, L. C. ve McRobbie, M. A. 2018. Ensuring the Integrity of Elections. Securing the Vote: Protecting American Democracy, National Academies of Sciences 103-105, USA.

Boneh, D., Goh, E.-J. ve Nissim, K. 2005. Evaluating 2-DNF Formulas on Ciphertexts. Theory of Cryptography, Springer, 325-341, Berlin, Germany.

Bosri, R., Uzzal, A. R., Omar, A. A., Hasan, A. S. M. T. ve Bhuiyan, Md. Z. A. 2019. Towards a Privacy-Preserving Voting System Through Blockchain Technologies. 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 5-8 August, 602-608. Fukuoka, Japan.

Bull, C., Gjøsteen, K. ve Nore, H. 2018. Faults in Norwegian internet voting. Third International Joint Conference on Electronic Voting E-Vote-ID, 2-5 October, 166-169, Bregenz, Austria.

Bulut, R., Kantarci, A., Keskin, S. ve Bahtiyar, S. 2019. Blockchain-Based Electronic Voting System for Elections in Turkey. 2019 4th International Conference on Computer Science and Engineering (UBMK), 11-15 September, 183-188, Samsun, Turkey.

Camenisch, J. ve Michels, M. 1998. A Group Signature Scheme Based on an RSA-Variant. BRICS Report Series, 5(27).

Cardillo, A. ve Essex, A. 2018. The Threat of SSL/TLS Stripping to Online Voting. E-Vote-ID 2018: Electronic Voting, Springer, 11143, 35-50, Berlin, Germany.

Castro, M. ve Liskov, B. 2002. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems, 20(4); 398-461.

Chaieb, M., Koscina, M., Yousfi, S., Lafourcade, P. ve Robbana, R. 2019. DABSTERS: Distributed Authorities using Blind Signature to Effect Robust Security in e-Voting: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, SCITEPRESS, 228-235, Prague, Czech Republic.

Chaum, D. ve van Heyst, E. 1991. Group Signatures. Advances in Cryptology—EUROCRYPT '9. Lecture Notes in Computer Science, Springer, 547, 257-265, Berlin, Germany.

Cheng, J.-C., Lee, N.-Y., Chi, C. ve Chen, Y.-H. 2018. Blockchain and smart contract for digital certificate. 2018 IEEE International Conference on Applied System Invention (ICASI), 13-17 April, 1046-1051, Chiba, Japan.

Chiang, L. 2009. Trust and security in the e-voting system. Electronic Government, an International Journal, 6(4); 343.

Clarke, D. ve Martens, T. 2016. E-voting in Estonia. Computer Science, ArXiv:1606.08654.

Cominetti, E. L. ve Simplicio, M. A. 2020. Fast Additive Partially Homomorphic Encryption From the Approximate Common Divisor Problem. IEEE Transactions on Information Forensics and Security, 15, 2988-2998.

Cranor, L. F. ve Cytron, R. K. 1997. Sensus: A security-conscious electronic polling system for the Internet. Proceedings of the Thirtieth Hawaii International Conference on System Sciences, 7-10 January, 561-570,Wailea, HI, USA.

Dagher, G. G., Marella, P. B., Milojkovic, M. ve Mohler, J. 2018. BroncoVote: Secure Voting System using Ethereum's Blockchain. Proceedings of the 4th International Conference on Information Systems Security and Privacy. SCITEPRESS. 96-107, Madeira, Portugal.

DeCusatis, C., Zimmermann, M. ve Sager, A. 2018. Identity-based network security for commercial blockchain services. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 8-10 January, 474-477, Las Vegas, USA.

Demestichas, K., Peppes, N., Alexakis, T. ve Adamopoulou, E. 2020. Blockchain in Agriculture Traceability Systems: A Review. Applied Sciences, 10(12); 4113.

Dimitriou, T. 2019. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting. Web Sitesi: https://eprint.iacr.org/2019/1406.pdf. Erişim Tarihi: 10.04.2020.

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C. ve Tan, K. L. 2017. BLOCKBENCH: A framework for analyzing private blockchains. Proceedings of the ACM SIGMOD International Conference on Management of Data, Part F1277, 1085-1100.

Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M. ve Wernsing, J. 2017. Manual for Using Homomorphic Encryption for Bioinformatics. Proceedings of the IEEE, 105(3); 1-16.

Dricot, L. ve Pereira, O. 2018. SoK: Uncentralisable Ledgers and their Impact on Voting Systems. Computer Science, ArXiv:1801.08064.

Elgamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4); 469-472.

Epstein, J. 2007. Electronic Voting. Computer, 40(8); 92-95.

Esteve, J. B., Goldsmith, B. ve Turner, J. 2012. International Experience with E-Voting. UK Parliament. Web Sitesi: https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf. Erişim Tarihi: 15.07.2020.

Fan, W., Kumar, S., Jadhav, V., Chang, S.-Y. ve Park, Y. 2021. A Privacy Preserving E-Voting System Based on Blockchain. Communications in Computer and Information Science, Springer, 1383, 148-159, Berlin, Germany.

Fan, X., Li, P., Zeng, Y. ve Zhou, X. 2020. Implement Liquid Democracy on Ethereum: A Fast Algorithm for Realtime Self-tally Voting System. Computer Science, ArXiv:1911.08774.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W. ve Wang, G. 2020. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. EURASIP Journal on Wireless Communications and Networking, 2020(1); 56.

Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. ve Colman, A. 2020. Blockchain Consensus Algorithms: A Survey. Computer Science, ArXiv:2001.07091.

Fink, R. A., Sherman, A. T. ve Carback, R. 2009. TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules. IEEE Transactions on Information Forensics and Security, 4(4); 628-637.

Fontaine, C. ve Galand, F. 2007. A Survey of Homomorphic Encryption for Nonspecialists. EURASIP Journal on Information Security, 2007, 1-10.

Fujioka, A., Okamoto, T. ve Ohta, K. 1993. A practical secret voting scheme for large scale elections. Advances in Cryptology—AUSCRYPT ’92, Springer, 718, 244-251, Berlin, Germany.

Fusco, F., Lunesu, M. I., Pani, F. E. ve Pinna, A. 2018. Crypto-voting, a Blockchain based e-Voting System. 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, SCITEPRESS, 3, 223-227, Seville, Spain.

Gao, S., Zheng, D., Guo, R., Jing, C. ve Hu, C. 2019. An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. IEEE Access, 7, 115304-115316.

Gentles, D. ve Sankaranarayanan, S. 2012. Application of Biometrics in Mobile Voting. International Journal of Computer Network and Information Security, 4(7); 57-68.

Gentry, C. 2009. A Fully Homomorphic Encryption Scheme. Dissertation. STOC '09: Proceedings of the forty-first annual ACM symposium on Theory of computing, May, 169-169.

Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P. ve Fierrez, J. 2017. Multi-biometric template protection based on Homomorphic Encryption. Pattern Recognition, 67, 149-163.

Goodman, R. ve Halderman, J. A. 2020. Internet Voting Is Happening Now. Web Sitesi: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html. Erişim Tarihi: 15.07.2020.

Gramoli, V. 2020. From blockchain consensus back to Byzantine consensus. Future Generation Computer Systems, 107, 760-769.

Grontas, P. ve Pagourtzis, A. 2019. Blockchain, consensus, and cryptography in

electronic voting. Homo Virtualis, 2(1); 79-79.

Gupta, Y., Shorey, R., Kulkarni, D. ve Tew, J. 2018. The applicability of blockchain in the Internet of Things. 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 3-7 January, 561-564, Bengaluru, India.

Gurubasavanna, M. G., Ulla Shariff, S., Mamatha, R. ve Sathisha, N. 2019. Multimode authentication based Electronic voting Kiosk using Raspberry Pi. Proceedings of the International Conference on I-SMAC, 30-31 August, Palladam, India.

Haber, S. ve Stornetta, W. S. 1991. How to time-stamp a digital document. Journal of Cryptology, 3(2); 99-111.

Hanifatunnisa, R. ve Rahardjo, B. 2017. Blockchain based e-voting recording system design. 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 26-27 October, 1-6, Lombok, Indonesia.

Hardwick, F. S., Gioulis, A., Akram, R. N. ve Markantonakis, K. 2018. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. Computer Science, ArXiv:1805.10258.

Haydaroğlu, C. ve Çevik, G. 2016. Türkiye'de Seçim Sistemlerinin Demokrasi Ve Ekonomi İlişkisi Çerçevesinde İncelenmesi. Uluslararası Politik Araştırmalar Dergisi, 2 (2. 1); 51-63.

He, Y., Li, H., Cheng, X., Liu, Y., Yang, C. ve Sun, L. 2018. A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications. IEEE Access, 6, 27324-27335.

Heiberg, S., Kubjas, I., Siim, J. ve Willemson, J. 2018. On Trade-offs of Applying Blockchains for Electronic Voting Bulletin Boards. International Association for Cryptologic Research. Web Sitesi: https://eprint.iacr.org/2018/685.pdf. Erişim Tarihi: 15.04.2020.

Hjálmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M. ve Hjalmtysson, G. 2018. Blockchain-Based E-Voting System. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2-7 July, 983-986, San Francisco, USA.

Holochain. 2022. Web Adresi: https://www.holochain.org/. Erişim Tarihi: 17.01.2022.

Hölbl, M., Kompara, M., Kamišalić, A. ve Nemec Zlatolas, L. 2018. A Systematic Review of the Use of Blockchain in Healthcare. Symmetry, 10(10); 470.

Ismail, L. ve Materwala, H. 2019. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry, 11(10).

Ismail, L. ve Materwala, H. 2020. Blockchain Paradigm for Healthcare: Performance Evaluation. Symmetry, 12(8); 1200.

Jardí-Cedó, R., Pujol-Ahulló, J., Castellà-Roca, J. ve Viejo, A. 2012. Study on poll-site

voting and verification systems. Computers & Security, 31(8); 989-1010.

Javed, M. U., Javaid, N., Aldegheishem, A., Alrajeh, N., Tahir, M. ve Ramzan, M. 2020. Scheduling Charging of Electric Vehicles in a Secured Manner by Emphasizing Cost Minimization Using Blockchain Technology and IPFS. Sustainability, 12(12); 5151.

Johnson, D. 2019. Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? European Journal of Risk Regulation, 10(2); 330-358.

Juels, A., Eyal, I. ve Naor, O. 2018. Blockchains won't fix internet voting security could make it worse. Web Sitesi: https://theconversation.com/blockchains-wont-fix-internet-voting-security-and-could-make-it-worse-104830. Erişim Tarihi: 03.04.2020.

Jung Hee Cheon ve Jinsu Kim. 2015. A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. IEEE Transactions on Information Forensics and Security, 10(5); 1052-1063.

Kaur, A., Nayyar, A. ve Singh, P. 2020. Blockchaın: A Path To The Future. Cryptocurrencies and Blockchain Technology Applications, Wiley, 1, 25-42.

Kaur, S., Chaturvedi, S., Sharma, A. ve Kar, J. 2021. A Research Survey on Applications of Consensus Protocols in Blockchain. Security and Communication Networks, 2021, 1-22.

Keshk, A. E. ve Abdul-Kader, H. M. 2007. Development of remotely secure e-voting system. 2007 ITI 5th International Conference on Information and Communications Technology, 16-18 December, 235-243, Cairo, Egypt.

Khan, K. M., Arshad, J. ve Khan, M. M. 2020. Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems, 105, 13-26.

Khelifi, A., Grisi, Y., Soufi, D., Mohanad, D. ve Shastry, P. V. S. 2013. M-Vote: A reliable and highly secure mobile voting system. Proceedings of the 2013 Palestinian International Conference on Information and Communication Technology, 15-16 April, 90-98, Gaza, Palestine.

Khoury, D., Kfoury, E. F., Kassem, A. ve Harb, H. 2018. Decentralized Voting Platform Based on Ethereum Blockchain. 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 14-16 November, 1-6, Beirut, Lebonan.

Kim, J. ve Yun, A. 2021. Secure Fully Homomorphic Authenticated Encryption. IEEE Access, 9, 107279-107297.

Kitsing, M. 2011. Online participation in Estonia: Active voting, low engagement. Proceedings of the 5th International Conference on Theory and Practice of

Electronic Governance—ICEGOV ’11, 26 - 29 September, 20, Tallinn, Estonia.

Kontogiannis, P. V. ve Varvarigou, T. 2019. ECDSA Private Keys Study of Security. OALib, 06(06); 1-20.

Kshetri, N. ve Voas, J. 2018. Blockchain-Enabled E-Voting. IEEE Software, 35(4); 95-99.

Lai, W.-J., Hsieh, Y., Hsueh, C.-W. ve Wu, J.-L. 2018. DATE: A Decentralized, Anonymous, and Transparent E-voting System. 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 15-17 August, 24-29, Shenzhen, China.

Latifi, S. Zhang, Y. and Cheng, L. C. 2019. Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market. 2019 IEEE International Conference on Blockchain, 14-17 July, 528-535, Atlanta, USA.

Lee, J., Choi, J., Kim, J. ve Oh, H. (2019). SAVER: SNARK-friendly, Additively-homomorphic, and Verifiable Encryption and decryption with Rerandomization. Web Adresi: https://eprint.iacr.org/2019/1270.pdf. Erişim Tarihi: 04.04.2020

Leonardos, S., Reijsbergen, D. ve Piliouras, G. 2019. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 14-17 May, 376-384, Seoul, South Korea.

Lewis, S. J., Pereira, O. ve Teague, V. 2019. The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system. Web Sitesi: https://www.digitale-gesellschaft.ch/uploads/2019/03/UniversalVerifiabilitySwissPost.pdf. Erişim Tarihi: 3.04.2020.

Li, H., Li, Y., Yu, Y., Wang, B. ve Chen, K. 2020. A Blockchain-based Traceable Self-tallying E-voting Protocol in AI Era. IEEE Transactions on Network Science and Engineering, 14(8).

Li, Jiaxing, Liu, Z., Chen, L., Chen, P. ve Wu, J. 2017. Blockchain-Based Security Architecture for Distributed Cloud Storage. 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), 12-15 December, 408-411, Guangzhou, China.

Li, Jing, Wang, X., Huang, Z., Wang, L. ve Xiang, Y. 2019. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. Journal of Parallel and Distributed Computing, 130, 91-97.

Li, X., Mei, Y., Gong, J., Xiang, F. ve Sun, Z. 2020. A Blockchain Privacy Protection Scheme Based on Ring Signature. IEEE Access, 8, 76765-76772.

Lin, I.-C. ve Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security, 19(5); 653-659.

Liu, Y. ve Wang, Q. 2017. An E-voting Protocol Based on Blockchain. Web Adresi: https://eprint.iacr.org/2017/1043.pdf. Erişim Tarihi: 13.04.2020.

Lone, A. H. ve Mir, R. N. 2019. Consensus protocols as a model of trust in blockchains. International Journal of Blockchains and Cryptocurrencies, 1(1); 7.

Luo, Y., Chen, Y., Chen, Q. ve Liang, Q. 2018. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. 2018 7th International Conference on Digital Home (ICDH), 30 November-1 December, 116-120, Guilin, China.

Lyu, J., Jiang, Z. L., Wang, X., Nong, Z., Au, M. H. ve Fang, J. 2019. A Secure Decentralized Trustless E-Voting System Based on Smart Contract. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 5-8 August, 570-577, Rotorua, New Zealand.

Mambo, M., Usuda, K. ve Okamoto, E. 1996. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM conference on Computer and communications security—CCS '96, 14-15 March, 48-57, New Delhi, India.

Matile, R., Rodrigues, B., Scheid, E. ve Stiller, B. 2019. CaIV: Cast-as-Intended Verifiability in Blockchain-based Voting. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 14-17 May, 24-28, Seoul, South Korea.

McCorry, P., Shahandashti, S. F. ve Hao, F. 2017. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. Financial Cryptography and Data Security, Springer, 10322, 357-375, Berlin, Heidelberg, Germany.

Mercer, R. 2016. Privacy on the Blockchain: Unique Ring Signatures. Computer Science, ArXiv:1612.01188.

Microsoft. 2021. Blockchain Technology and Applications. Web Adresi: https://azure.microsoft.com/en-us/solutions/blockchain/. Erişim Tarihi: 01.09.2021.

Microsoft Seal. 2021. Seal Homomorphic Encrytion. Web Adresi: https://www.microsoft.com/en-us/research/project/microsoft-seal/. Erişim Tarihi: 09.11.2021.

Mohanta, B. K., Jena, D., Panda, S. S. ve Sobhanayak, S. 2019. Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things, 8, 100107-100107.

Murtaza, M. H., Alizai, Z. A. ve Iqbal, Z. 2019. Blockchain Based Anonymous Voting System Using zkSNARKs. 2019 International Conference on Applied and Engineering Mathematics (ICAEM), 27-29 August, 209-214, Taxila, Pakistan.

Na, S. ve Park, Y. B. 2018. Web-based Nominal Group Technique Decision Making Tool Using Blockchain. 2018 International Conference on Platform Technology and Service (PlatCon), 29-31 January, 1-6, Jeju, South Korea.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Web Sitesi: https://bitcoin.org/bitcoin.pdf. Erişim Tarihi: 02.11.2019.

Nasir, Q., Qasse, I. A., Abu Talib, M. ve Nassif, A. B. 2018. Performance Analysis of Hyperledger Fabric Platforms. Security and Communication Networks, 2018, 1-14. doi:10.1155/2018/3976093

Noizat, P. 2015). Blockchain Electronic Vote. Handbook of Digital Currency, Elsevier, 453-461.

Ogburn, M., Turner, C. ve Dahal, P. 2013. Homomorphic Encryption. Procedia Computer Science, 20, 502-509.

Olumide S., A., Olutayo K., B. ve E. Adekunle, S. 2020. A Review of Electronic Voting Systems: Strategy for a Novel. International Journal of Information Engineering and Electronic Business, 12(1); 19-29.

Oo, H. N. ve Aung, A. M. 2014. A Survey of Different Electronic Voting Systems. International Journal of Scientific Engineering and Technology Research (IJSETR), 03(16); 3460-3464.

Ortega, A. P., Marcos, X. E., Chiang, L. D. ve Abad, C. L. 2009. Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt. 2009 Latin American Network Operations and Management Symposium, 19-21 October, 1-9, Punta del Este, Uruguay.

Osgood, R. 2016. The Future of Democracy: Blockchain Voting. Web Sitesi: http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf. Erişim Tarihi: 26.06.2020.

Osmanoglu, M., Tugrul, B., Dogantuna, T. ve Bostanci, E. 2020. An Effective Yield Estimation System Based on Blockchain Technology. IEEE Transactions on Engineering Management, 1-12.

Paar, C. ve Pelzl, J. 2010. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 1-27, Berlin, Heidelberg, Germany.

Paillier, P. 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Advances in Cryptology—EUROCRYPT ’99, Springer, 1592, 223-238, Berlin, Heidelberg, Germany.

Palas Nogueira, J. ve de Sá-Soares, F. 2012. Trust in e-Voting Systems: A Case Study. Knowledge and Technologies in Innovative Information Systems, Springer, 129, 51-66, Berlin, Heidelberg, Germany.

Park, S., Specter, M., Narula, N. ve Rivest, R. L. 2020. Going from Bad to Worse: From

Internet Voting to Blockchain Voting. Web Sitesi: https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf. Erişim Tarihi: 17.07.2020.

Pathak, A., Wasay, A., Singh, C., Bhavan, R. ve Umale, J. 2018. Design and implementation of a secure and robust voting system based on blockchain. International Journal of Advance Research, Ideas and Innovations in Technology, 4(5); 869-875.

Pawlak, M. ve Poniszewska-Marańda, A. 2021. Trends in blockchain-based electronic voting systems. Information Processing & Management, 58(4); 102595.

Peng, H.-T., Hsu, W. W. Y., Ho, J.-M. ve Yu, M.-R. 2016. Homomorphic encryption application on FinancialCloud framework. 2016 IEEE Symposium Series on Computational Intelligence (SSCI) 6-9 December, 1-5, Athens, Greece.

Peng, K., Aditya, R., Boyd, C., Dawson, E. ve Lee, B. 2004. Multiplicative Homomorphic E-Voting. A. Progress in Cryptology—INDOCRYPT 2004, Springer, 3348, 61-72, Berlin, Heidelberg, Germany.

Peters, G. W. ve Panayi, E. 2016. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Banking Beyond Banks and Money, Springer, 239-278, Berlin, Heidelberg, Germany.

Petersen, K., Feldt, R., Mujtaba, S. ve Mattsson, M. 2008. Systematic mapping studies in software engineering. EASE'08: Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering, 26-27 June, 68-77, Swindon, United Kingdom.

Pilkington, M. 2015. Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, SSRN, 2662660, Rochester, NY, USA.

Raikwar, M., Mazumdar, S., Ruj, S., Sen Gupta, S., Chattopadhyay, A. ve Lam, K.-Y. 2018. A Blockchain Framework for Insurance Processes. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 26-28 Feburary, 1-4, Paris, France.

Riemann, R. ve Grumbach, S. (2017). Distributed Protocols at the Rescue for Trustworthy Online Voting. Proceedings of the 3rd International Conference on Information Systems Security and Privacy, SciTePress, 1, 499-505.

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

Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., ve Zhe Xia. (2009). PrÊt À Voter: A Voter-Verifiable Voting System. IEEE Transactions on Information Forensics and Security, 4(4); 662-673.

Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D. ve Mohaisen, A. 2019. Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain

Systems. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 14-17 May, 285-292, Seoul, South Korea.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. ve Mohaisen, A. 2019a. Exploring the Attack Surface of Blockchain: A Systematic Overview. Computer Science, ArXiv:1904.03487.

Sabry, S. S., Kaittan, N. M. ve Majeed, I. 2019. The road to the blockchain technology: Concept and types. Periodicals of Engineering and Natural Sciences (PEN), 7(4); 1821-1832.

Sadia, K., Masuduzzaman, M., Paul, R. K. ve Islam, A. 2019. Blockchain Based Secured E-voting by Using the Assistance of Smart Contract. Computer Science, ArXiv:1910.13635.

Sadouskaya, K. 2017. Adoption of Blockchain Technology in Supply Chain and Logistics. Thesis. XAMK South-Eastern Finland University of Applied Sciences, Finland.

Salarifard, R. ve Bayat-Sarmadi, S. 2019. An Efficient Low-Latency Point-Multiplication Over Curve25519. IEEE Transactions on Circuits and Systems I: Regular Papers, 66(10); 3854-3862.

Saproo, S., Warke, V., Pote, S. ve Dhumal, R. 2020. Online Voting System using Homomorphic Encryption. ITM Web of Conferences, 32, 03023.

Sathya, V., Sarkar, A., Paul, A. ve Mishra, S. 2019. Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 27-29 March, 1075-1079, Erode, India.

Schiedermeier, M., Hasan, O., Mayer, T., Brunie, L. ve Kosch, H. 2019. A transparent referendum protocol with immutable proceedings and verifiable outcome for trustless networks. Computer Science, ArXiv:1909.06462.

Sedky, M. H. ve Ramzy Hamed, E. M. 2015. A secure e-Government's e-voting system. 2015 Science and Information Conference (SAI), 28-30 July, 1365-1373, London, UK.

Shahnaz, A. Qamar, U. and Khalid, A. 2018. Using Blockchain for Electronic Health Records. IEEE Access, 7; 147782–147795.

Shahzad, B. ve Crowcroft, J. 2019. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access, 7, 24477-24488.

Shakhbulatov, D. Arora, A. Dong, Z. and Rojas-Cessa. 2019. Blockchain Implementation for Analysis of Carbon Footprint across Food Supply Chain. 2019 IEEE International Conference on Blockchain, 14-17 July 2019, 546-551, Atlanta, USA.

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

Shen, C. ve Pena-Mora, F. 2018. Blockchain for Cities—A Systematic Literature Review. IEEE Access, 6, 76787-76819.

Shrestha, R. ve Kim, S. 2019. Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities. Advances in Computers, Elsevier, 115, 293-331, Amsterdam, The Netherlands.

Shukla, S., Thasmiya, A. N., Shashank, D. O. ve Mamatha, H. R. 2018. Online Voting Application Using Ethereum Blockchain. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 19-22 September, 873-880, Bangalore, India.

Silva, R. A., Senger de Souza, S. do R. ve Lopes de Souza, P. S. 2017. A systematic review on search based mutation testing. Information and Software Technology, 81, 19-35.

Singh, S., Sanwar Hosen, A. S. M. ve Yoon, B. 2021. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. IEEE Access, 1-1.

Solat, S. 2019. RDV: An Alternative To Proof-of-Work And A Real Decentralized Consensus For Blockchain. Computer Science, ArXiv:1707.05091.

Specter, M. A., Koppel, J. ve Weitzner, D. 2020. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Web Sitesi: https://www.usenix.org/conference/usenixsecurity20/presentation/specter. Erişim Tarihi: 11.03.2020.

Srivastava, G., Dhar Dwivedi, A. ve Singh, R. 2018. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, 26-28 July, 674-679, Porto, Portugal.

Stone, J. 2019. Backdoor discovered in Swiss voting system would have allowed hackers to alter votes. Cyberscoop. Web Sitesi: https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/. Erişim Tarihi: 03.04.2020.

Sudharsan, B., Tharun, R. V., Krishna, N. M. P., Raj, B. J., Arvindh, S. M. ve Alagappan, M. 2019. Secured Electronic Voting System Using the Concepts of Blockchain. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 17-19 October, 0675-0681, Vancouver, Canada.

Sun, G., Dai, M., Sun, J. ve Yu, H. 2021. Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain. IEEE Internet of Things Journal, 8(8); 6257-6272.

Sun, X., Wang, Q. ve Kulicki, P. 2019. A Simple Voting Protocol on Quantum Blockchain. International Journal of Theoretical Physics, 58(1); 275-281.

Susskind, J. 2017. Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System. San Diego Law Review, 54(4); 785-821.

Swathi, P., Modi, C. ve Patel, D. 2019. Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 6-8 July, 1-6, Kanpur, India.

Tan, B. Q., Wang, F., Liu, J., Kang, K. ve Costa, F. 2020. A Blockchain-Based Framework for Green Logistics in Supply Chains. Sustainability, 12(11); 4656.

Tan, S.-Y., Yeow, K.-W. ve Hwang, S. O. 2019. Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things. IEEE Internet of Things Journal, 6(4); 6384-6395.

Tang, H., Shi, Y. ve Dong, P. 2019. Public blockchain evaluation using entropy and TOPSIS. Expert Systems with Applications, 117, 204-210.

Tarasov, P. ve Tewari, H. (2017). Internet Voting Using Zcash. Web Sitesi: https://eprint.iacr.org/2017/585.pdf. Erişim Tarihi: 12.03.2020.

Taş, R., and Tanrıöver, Ö. Ö. 2020. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry 2020, 12(8); 1328.

Teja, K., Shravani, M., Simha, C. Y. ve Kounte, M. R. 2019. Secured voting through Blockchain technology. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 23-25 April, 1416-1419, Tirunelveli, India.

Thuy, L. V.-C.-, Cao-Minh, K., Dang-Le-Bao, C. ve Nguyen, T. A. 2019. Votereum: An Ethereum-Based E-Voting System. 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), 20-22 March, 1-6, Danang, Vietnam.

Trechsel, A. H., Kucherenko, V., Silva, F. ve Gasser, U. 2016. Potential And Challenges Of E-Voting In The European Union. Brussels: European Union. Edu Report 2016/11; Frenza, Italy.

Truffle Suite. 2021.Tuffle Documantation. Web Sitesi: https://www.trufflesuite.com/docs. Erişim Tarihi: 17.09.2020.

Tso, R., Liu, Z.-Y. ve Hsiao, J.-H. 2019. Distributed E-Voting and E-Bidding Systems Based on Smart Contract. Electronics, 8(4); 422.

Turkanović, M. Hölbl, M. Košič, K. Heričko, M. and Kamišalić, A. 2018. EduCTX: A Blockchain-Based Higher Education Credit Platform. IEEE Access, 6; 5112 – 5127.

Türk, H. S. Seçim, 2006. Seçim Sistemleri ve Anayasal Tercih. Anayasa Yargısı. Web Sitesi: https://www.anayasa.gov.tr/Files/Pdf/Anayasa_Yargisi/Anyarg23/Turk.Pdf. Erişim Tarihi: 11.04.2020.

Vegendla, A., Duc, A. N., Gao, S. ve Sindre, G. 2018. A Systematic Mapping Study on Requirements Engineering in Software Ecosystems. Journal of Information Technology Research, 11(1); 49-69.

Venkatapur, Rekha. B., Prabhu, B., Navya, A., Roopini, R. ve Niranjan, S. A. 2018. Electronic Voting Machine Based On Blockchain Technology and Aadhar Verification. International Journal of Innovations in Engineering and Science, 3, 12-15.

Villegas-Ch, W., Palacios-Pacheco, X. ve Román-Cañizares, M. 2020) Integration of IoT and Blockchain to in the Processes of a University Campus. Sustainability, 12(12); 4970.

Volkamer, M. ve McGaley, M. 2007. Requirements and evaluation procedures for eVoting. Proceedings—Second International Conference on Availability, Reliability and Security, ARES 2007, 10-13 April, 895-902, Vienna, Austria.

Wang, B., Li, Z. ve Li, H. 2020. Hybrid consensus algorithm based on modified proof-of-probability and DPoS. Future Internet, 12(8); 1-17.

Wang, B., Sun, J., He, Y., Pang, D. ve Lu, N. 2018. Large-scale Election Based On Blockchain. Procedia Computer Science, 129, 234-237.

Wang, H., Wang, Y., Cao, Z., Li, Z. ve Xiong, G. 2019. An Overview of Blockchain Security Analysis. Communications in Computer and Information Science, Springer, 970, 55-72, Singapore

Water, G. V. 2017. Blockchaın Ballot Electoral Enhancement or Danger to Democracy?. Master's Thesis. Tilburg Universty. Tilburg, Netherlands.

Xiao, Y., Zhang, P. ve Liu, Y. 2021. Secure and Efficient Multi-Signature Schemes for Fabric: An Enterprise Blockchain Platform. IEEE Transactions on Information Forensics and Security, 16, 1782-1794.

Xie, J. Tang, H. Huang, T. Yu, F. R. Xie, R. Liu, J. and Liu, Y. 2019. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys & Tutorials, 21 (3); 2794 – 2830.

Yahaya, A. S., Javaid, N., Alzahrani, F. A., Rehman, A., Ullah, I., Shahid, A. ve Shafiq, M. 2020. Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism. Sustainability, 12(8); 3385.

Yan, X., Wu, Q. ve Sun, Y. 2020. A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. Wireless Communications and Mobile Computing, 2020(i); 1-9.

Yang, X., Yi, X., Nepal, S., Kelarev, A. ve Han, F. 2018. A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption. IEEE Access, 6, 20506-20519.

Yavuz, E., Koc, A. K., Cabuk, U. C. ve Dalkilic, G. 2018. Towards secure e-voting using ethereum blockchain. 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 22-25 March, 1-7, Antalya, Turkey.

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q. ve Choo, K.-K. R. 2020. An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. IEEE Transactions on Services Computing, 13(4); 625-638.

Yi, O. K. ve Das, D. (2020). Block Chain Technology For Electronic Voting. Journal of critical reviews, 7(03).

Yu, B., Liu, J., Amin, S., Nepal, S., Steinfeld, R., Rimba, P. ve Au, M. H. 2018. Platform-independent Secure Blockchain-Based Voting System. Web Sitesi: https://eprint.iacr.org/2018/657.pdf. Erişim Tarihi: 17.04.2020.

Yuan, Y. ve Wang, F.-Y. 2016. Towards blockchain-based intelligent transportation systems. 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 1-4 November, 2663-2668, Rio de Janeiro, Brazil.

Zaghloul, E., Li, T., Mutka, M. W. ve Ren, J. 2020. Bitcoin and Blockchain: Security and Privacy. IEEE Internet of Things Journal, 7(10); 10288-10313.

Zhang, D. 2020. Methods and Rules of Voting and Decision: A Literature Review. Open Journal of Social Sciences, 08(01); 60-72.

Zhang, Q., Xu, B., Jing, H. ve Zheng, Z. 2019. Ques-Chain: An Ethereum Based E-Voting System. Computer Science, ArXiv:1905.05041.

Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A. ve Huang, S. 2018. A Privacy-Preserving Voting Protocol on Blockchain. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2-7 July, 401-408, San Francisco, USA.

Zhao, Z. ve Chan, T.-H. H. (2016). How to Vote Privately Using Bitcoin. Information and Communications Security, Springer, 9543, 82-96, Berlin, Heidelberg, Germany.

Zheng Wei, C. C. ve Wen, C. C. 2018. Blockchain-Based Electronic Voting Protocol. JOIV : International Journal on Informatics Visualization, 2(4-2); 336-336.

Zheng, Z., Xie, S., Dai, H. N., Chen, X. ve Wang, H. 2018. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4); 352.