T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOK ZİNCİRİ TABANLI GERÇEK ZAMANLI ÇEVRİMİÇİ OYLAMA SİSTEMİ ÖNERİSİ

YÜKSEK LİSANS TEZİ

Ufuk ALYAZ

Bilgisayar Mühendisliği Ana Bilim Dalı
Bilgisayar Mühendisliği Programı

Ocak, 2021

T.C.

İSTANBUL AYDIN ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOK ZİNCİRİ TABANLI GERÇEK ZAMANLI ÇEVRİMİÇİ OYLAMA SİSTEMİ ÖNERİSİ

YÜKSEK LİSANS TEZİ

UFUK ALYAZ

(Y1713.010032)

Bilgisayar Mühendisliği Ana Bilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ali GÜNEŞ

Ocak, 202

YEMİN METNİ

Yüksek Lisans tezi olarak “Blok Zinciri Tabanlı Gerçek Zamanlı Çevrimiçi Oylama Sistemi Önerisi” konulu çalışmamın, tezin analizinden sonuçlandırılmasına kadar geçen süreçlerde bilimsel ahlak ve geleneklerine aykırı düşecek bir durum olmaksızın hazırlandığını ve yararlandığım eserlerin Kaynakça’da yer aldığını ve atıf yapılarak yararlanılmış olduğunu beyan ederim (Ocak 2021).

Ufuk ALYAZ

ÖNSÖZ

Bu çalışmanın amacı; blok zinciri ve WebRTC gerçek zamanlı iletişim teknolojilerinin birlikte kullanılacağı merkezi otoriteye bağlı olmayan dağıtık yapıda çevrimiçi oylama sistem önerisidir.

Danışmanım Prof. Ali GÜNEŞ'e yüksek lisans eğitimime desteği ile her zaman tüm samimiyetiyle akıl hocalığı yaptığı için teşekkür ederim.

Son olarak bana destek veren, cesaretlendiren, her zaman yanımda olduklarını hissettiğim sevgili ailem ve arkadaşlarıma teşekkür ederim.

Ocak 2021 **Ufuk ALYAZ**

İÇİNDEKİLER

KISALTMALAR

P2P **:** Peer to Peer (Kişiden kişiye)

B2B **:** Business to Business (İşletmeden işletmeye)

RPoW **:** Yeniden Kullanılabilir İş İspatı

RSA **:** Rivest - Shamir - Adleman

PoW **:** Proof of Work (İş İspatı)

PoS **:** Proof of Stake (Hisse İspatı)

DPoS **:** Delegated Proof of Stake (Yetkilendirilmiş Hisse İspatı)

JS **:** Javascript

RTC **:** Real Time Communication (Gerçek zamanlı iletişim)

API **:** Application Programming Interface (Uygulama programlama arayüzü)

XHR : XMLHttpRequest

SSE : Server-Sent Events

WS : Web Socket

HTTP **:** Hypertext Transport Protocol (Yüksek metin aktarım protokolü)

TLS **:** Transport Layer Security (Aktarım katmanı güvenliği)

TCP **:** Transport Control Protocol (Aktarım kontrol protokolü)

IP : Internet Protocol (İnternet protokolü)

SRTP **:** Secure Real-Time Transport Protocol (Güvenli gerçek zamanlı aktarım protokolü)

SCTP **:** Stream Control Transport Protocol (Akış kontrol aktarım protokolü)

DLTS **:** Datagram Transport Layer Security (Veribloğu aktarım katmanı güvenliği)

ICE **:** Interactive Connectivity Establishment (Etkileşimli bağlantı kurulumu)

STUN **:** Secure Real Time Transport Protocol (Gerçek zamanlı güvenli aktarım

TURN **:** Traversal Using Relays Around NAT (NAT etrafındaki roleler arasındaki geçiş)

SDP **:** Session Description Protocol (Oturum tanımlama protokolü)

UDP **:** User Datagram Protocol (Kullanıcı veribloğu protokolü) protokolü)

SMS **:** Short Message Service (Kısa mesaj hizmeti)

SHA **:** Secure Hash Algorithm (Güvenli karma algoritma)

DApp **:** Decentralized application (Merkezi olmayan uygulama)

TANIMLAMALAR

Transaction **:** Süreç

Public **:** Açık

Secret **:** Gizli

Client **:** İstemci

Server **:** Sunucu

Spam **:** İstenmeyen

Signaling **:** Sinyalleşme

Network : Ağ

ŞEKİL LİSTESİ

TABLO LİSTESİ

BLOK ZİNCİRİ TABANLI GERÇEK ZAMANLI ÇEVRİMİÇİ OYLAMA SİSTEMİ ÖNERİSİ

ÖZET

Çağın getirisi olarak çevrimiçi sistemler üzerinden hemen her iş daha etkili ve daha hızlı yapılabilmektedir. Türkiye genelinde %90,7 oranında hane halkının evden internete erişim sağlamasıyla, gelişen teknoloji ve işlem kapasiteleri ile günlük hayatımızın büyük bir kısmında dijital dönüşüm gerçekleştirmeye devam etmektedir. Bazı alanlarda ise güvenlik nedeniyle dijital dönüşüm süreci tamamlanamamıştır. Bunlardan biri de internet tabanlı oylama (seçim) sistemleridir. Seçimler gelişmiş toplumların demokrasisinin ilk adımıdır. Merkezi yapıya sahip geleneksel sistemler tek bir otorite kontörlünde bulunup, manipüle edilmesi kolay olduğu için dijitalleşme sürecine dâhil olmamıştır. Kripto para birimleri ile gündeme gelen ve son yıllarda teknolojisi anlaşıldıkça daha da popüler olan blok zinciri teknolojisi değiştirilemeyen, dağıtık yapısı, zaman damgalı kronolojik ve şifrelenmiş blok oluşturma mekanizması sayesinde bu süreç ile seçimlerin dijitale dönüşmesi yeniden hız kazanmıştır. Bu çalışmada veri karıştırma algoritmaları ile eşlerin iletişiminin herhangi bir sunucu üzerinden olmayıp eşten eşe bağlı olarak, kripto para birimleri kullanılmadan, birbirine bağlı olan eşler arası dağıtık blok zinciri sistem mimarisi kurgulanmıştır. Bu kurgu, katılımcıların birbirine gerçek zamanlı iletişim (WebRTC) üzerinde bağlı ve aynı zamanda konum olarak birbirinden bağımsız, uzakta olmasına da olanak vermektedir. Blok zinciri ve gerçek zamanlı iletişim (RTC) teknolojileri birlikte kullanılarak çağın gereksinimi olan güvenli, merkezi olmayan dağıtık yapıda, gerçek zamanlı, planlama ve uygulama maliyet düşük, esnek ve çevik çevrimiçi seçim oylama sistemi önerilmektedir.

Anahtar Kelimeler: *Blok zinciri, RTC, Gerçek zamanlı sistemler, Dağıtık sistemler, Çevrimiçi oylama sistemleri*

BLOCKCHAIN-BASED REAL-TIME ONLINE VOTING SYSTEM PROPOSAL

ABSTRACT

As a result of the times, almost every job can be done more effectively and faster through online systems. In Turkey, the rate of gaining access to the internet from home 90.7% of households in a large part of our daily lives by developing technology and processing capacity continues to perform digital conversion. In some areas, the digital transformation process could not be completed due to security reasons. One of them is internet-based voting (election) systems. Elections are the first step in the democracy of developed societies. Traditional systems with a central structure are not included in the digitalization process because they are available with a single authority and are easy to manipulate. The blockchain technology, which has come to the fore with crypto currencies and has become more popular as its technology is understood in recent years, has gained momentum with this process, thanks to its distributed structure, time stamped chronological and encrypted block generation mechanism. In this study, a peer-to-peer distributed block chain system architecture, which is connected to each other without using crypto currencies, has been designed with data scrambling algorithms. This setup allows the participants to be connected to each other via real-time communication (WebRTC) and at the same time independent from each other in terms of location. Using blockchain and real-time communication (RTC) technologies together, a secure, decentralized distributed structure, real-time, low planning and implementation cost, flexible and agile online election voting system is proposed.

Keywords: *Blockchain, RTC, Real-time systems, Distributed systems, Online voting systems*

1. GİRİŞ

Son yıllarda popülerliğini daha da artırmış olan blok zincirinin; teknolojisi anlaşıldıkça, ilgi odağına haline gelmesi ile birçok sektörde olduğu gibi kurum/kuruluşların dijitalleşme sürecinde en büyük katkıyı sağlayacak potansiyele sahip olduğu ortaya çıkmıştır. Verinin depolanma teknolojisi olan blok zinciri, verinin tutulduğu her bir bloğun zaman damgası ile kendinden önceki bloğun da özet bilgisini kısaca "hash" değerini ve kendi verisinin hash değerini tutacak şekilde kronolojik sırayla birbirlerine eklenerek oluşturulmasıdır. Gözün renkli kısmı olan irisin benzersiz oluşu ve ölene kadar asla değişmemesi [1] gibi blok zincirinin içerisinde bir önceki bloğun hash değerinin değişmemesi aynıdır. Sağlıklı bir blok zincirinde son bloktan başlayarak ilk bloğa kadar doğrulama yapılabilir.

Hash, bloğun veri bütünlüğü ile oluşturulduğundan dışarıdan herhangi bir müdahale edilmesi hash değerinin değişmesine neden olup zinciri bozacaktır. Teoride bu değişiklik ilgili blok baz alınarak kendinden sonraki blokları değiştirerek mümkündür. Şu ana kadar aynı yapıya sahip görünüyor olsa da blok zincirinin en büyük avantajı merkezi yapıya sahip olmadan dağıtık olarak uygulanıyor olmasıdır. Kısaca blok zincir defteri tek bir noktada değil ağa bağlı olan herkes (düğüm) tarafından tutulmaktadır. Bu belirgin özelliği blok zinciri ağlarına saldırı maliyetini artırmakla birlikte pratikte mümkün değildir. Yeni bir bloğun eklenme isteği sistemde yer alan tüm düğümler tarafından onay verilmesi dâhilinde tamamlanabilir. Herhangi bir düğümde değişiklik, bozulma meydana gelirse, o düğüm %51 oranında sistemdeki diğer düğümler tarafından kontrol edilir ve yok edilerek sağlam bir şekilde defter ile güncellenir [2]. Kontrol oranı ne kadar %100'e yakın olursa sistemin güvenlik zafiyeti o kadar azalacaktır.

Özetle blok zinciri yapısal olarak üzerinde yer alan her bir verinin kendisinden önceki bloğun özet şifresi (hash) ile yeni bir bloğu kronolojik olarak kayıt altına alan bir veri yönetim sistemidir [3]. Satoshi Nakamoto'nun "Bitcoin: A Peer-to-Peer Electronic Cash System" makalesinden bu sistemin blok zinciri olduğu anlaşılmaktadır [4].

WebRTC gerçek zamanlı iletişim projesi Google tarafından 2011 yılında açık kaynaklı olarak tanıtılmıştır. Kullanıcılar arası bire-bir (peer-to-peer) bağlantı olarak veri, ses ve görüntü paylaşımını herhangi bir medya sunucusuna gerek duymadan sağlayabilmektedir.

Adil ve demokratik bir sisteminde oy kullanılması için sistemin barındırması gereken ölçütler: Yeterlilik ve doğrulama, güvenilirlik, bütünlük, şeffaflık ve denetime açıklık, gizliliğin korunması ve baskı altına alınabilmesinin önlenmesi, esneklik, kolaylık, onaylanabilme ve makul maliyetidir [5].

Bu çalışmada blok zinciri, WebRTC ile dağıtık yapıda kullanılabilecek güvenilir, şeffaf, manipüle edilmesinin maliyeti fazla olan sistem yaklaşımı gösterilmiştir. Mevcut yaklaşımlardan farklı olarak blok zinciri veri yönetim mantığını, WebRTC gerçek zamanlı teknolojisi ile birleştirerek oy kullanım ölçütlerini karşılayan çevrimiçi oylama sistem önerisi yapılmıştır.

1.1 Araştırma Problemi

Türkiye genelinde %90,7 oranında evden internete erişim sağlamasıyla, gelişen teknoloji ve işlem kapasiteleri ile günlük hayatımızın büyük bir kısmında dijital dönüşüm gerçekleştirmeye devam etmektedir. Bazı alanlarda ise güvenlik nedeniyle dijital dönüşüm süreci tamamlanamamıştır. Bunlardan biri de internet tabanlı oylama (seçim) sistemleridir. Seçimler gelişmiş toplumların demokrasisinin ilk adımıdır. Merkezi yapıya sahip geleneksel sistemler tek bir otorite kontörlünde bulunup, manipüle edilmesi kolay olduğu için dijitalleşme sürecine dâhil olmamıştır. Son yıllarda teknolojisi anlaşıldıkça daha da popüler olan blok zinciri teknolojisi değiştirilemeyen, dağıtık yapısı, zaman damgalı kronolojik ve şifrelenmiş blok oluşturma mekanizması sayesinde bu süreç ile seçimlerin dijitale dönüşmesi yeniden hız kazanmıştır.

Yerel ve ülke geneli seçimler akla ilk gelen olsa da bazı organizasyon yapılarında, örneğin; site yönetimleri, vakıflar, dernekler, kulüpler, sivil toplum örgütleri vb. kuruluşların yöneticilerinin belirlenmesinde de seçimler uygulanmaktadır. Seçimler gelişmiş toplumların demokrasisinin ilk adımıdır. Merkezi yapıya sahip geleneksel sistemler tek bir otorite kontörlünde bulunup, manipüle edilmesi kolay olduğu için dijitalleşme sürecine dâhil olmadıkları gözlemlenmiştir.

1.2 Araştırmanın Amacı

Blok zinciri altyapısı ile dağıtık olarak ülke geneli veya yerel seçimler olmak üzere, referandum, site yönetimleri, vakıflar, dernekler, kulüpler, sivil toplum örgütleri vb. kuruluşların nezdinde çevrimiçi oylama sistemlerinin uygulanabileceği gözlemlenmiştir. Kripto para birimleri ile gündeme gelen ve son yıllarda teknolojisi anlaşıldıkça daha da popüler olan blok zinciri teknolojisi değiştirilemeyen, dağıtık yapısı, zaman damgalı kronolojik ve şifrelenmiş blok oluşturma mekanizması sayesinde bu süreç ile seçimlerin dijitale dönüşmesi yeniden hız kazanmıştır. Veri karıştırma algoritmaları ile eşlerin iletişiminin herhangi bir sunucu üzerinden olmayıp eşten eşe bağlı olarak, kripto para birimleri kullanılmadan, birbirine bağlı olan eşler arası dağıtık blok zinciri sistem mimarisi kurgulanmıştır.

Bu kurgu, katılımcıların birbirine gerçek zamanlı iletişim (WebRTC) üzerinde bağlı ve aynı zamanda konum olarak birbirinden bağımsız, uzakta olmasına da olanak vermektedir. Blok zinciri ve gerçek zamanlı iletişim (RTC) teknolojileri birlikte kullanılarak çağın gereksinimi olan güvenli, merkezi olmayan dağıtık yapıda, gerçek zamanlı, planlama ve uygulama maliyet düşük, esnek ve çevik çevrimiçi seçim oylama sistemi önerilmektedir.

1.3 Varsayımlar

Bu çalışma; aşağıdaki varsayımların tamamlandığı düşünülerek hazırlanmıştır.

- Oylama sisteminin tanımlaması ve seçmenlerin belirlenmiş olması,
- Oylama sistemi için seçmenlerin bir akıllı mobil cihaz kullanıyor olması,
- Oylama sistemi için akıllı mobil cihazın internete bağlı olması,
- Seçmenlerin kendi giriş bilgileri ile sisteme giriş yapıp yetkilendirme alabilmesi,
- Seçmenlerin baskı altında olmadan hür iradeleri ile tercihlerinin yapıyor olması

2. BENZER ÇALIŞMALAR

Yapılan araştırmalarda blok zinciri tabanlı oy kullanma uygulamaları internet üzerinde araştırılmış, konu ile alakalı mevcut uygulamaların çok sınırlı olduğu gözlemlenmiştir.

2.1 We Vote

WE vote, web tabanlı Waves blok zinciri üzerinde Ride dili kullanılarak hazırlanan akıllı sözleşmeler ile bireylerin sahip oldukları varlıkları transfer etmek amacıyla kullanılmaktadır. Blok zinciri üzerinde Web 3.0 uygulamalarını merkezi olmayan şekilde dağıtık olarak çözüm altyapısı sağlamaktadır. Waves blok zincirindeki işlemler WavesCoin kullanarak tamamlanmaktadır. WavesCoin, Bitcoin gibi açık kaynak kodludur ve kripto para birimidir [6]. Rusya'da telekomünikasyon şirketi olan Rostelecom iş birliği ile 13-20 Eylül 2020 tarihlerinde Rusya'nın Kursk ve Yaroslavl bölgelerinde kullanılmıştır. Genel olarak 36 binden fazla katılımcı sayısı, %90'ın üzerinde de katılımcı oranı ile tamamlanmıştır.

2.2 Polys

Polys, web üzerinde çalışan, RUST dili kullanılarak yazılmış "Exonum Blockchain Framework" kullanılarak oluşturulmuştur. Exonum Framework; yapılan işlemleri Bitcoin ağına katılım için kolaylık sağlayan bir araçtır. Bu doğrultuda Polys ile yapılan işlemler direkt olarak Bitcoin ağında yer almaktadır [7]. Rusya içerisinde Volgograd bölgesinde katılımcı bütçeleme oylama etkinliğine 185.000'den fazla kişi insiyatif bütçeleme projelerine oy vermiştir [8].

2.3 Inno Vote

Inno Vote web üzerinde dağıtık blok zinciri alt yapısını "The BallotChain" ile desteklemektedir. Kripto para alt birimi olan token kullanılmaktadır. Her bir token bir ID'ye sahiptir [9] ve seçmene verilir, ağ üzerinde kullanılan her bir token oy pusulası olarak yer almaktadır.

2.4 Voatz

Voatz blok zinciri ve aynı zamanda biometrik doğrulama da yaparak yetkilendirme veren bir platformdur. Mobil ve tablet üzerinde aktivasyon doğrulaması ile çalışmaktadır. IBM'in geliştirdiği Hyperledger Fabric'ten blok zinciri gücünü almaktadır [10]. İlk olarak ABD'de askeri alanda West Virginia ardından Denver ve UTAH Country kullanmıştır [11].

2.5 Zug ID ile Ethereum Ağında İsviçre'de Oy Kullanım

İsviçre Zug şehrinde ikamet eden kullanıcının uPort mobil uygulaması ile Ethereum ağına dâhil olması ile benzersiz tekil kullanıcı niteliği kazanmaktadır. Gerekli olan yetkilendirme alındıktan sonra ancak kullanıcı çevrimiçi oylamaya katılabilmektedir. Dijital kimlik sayesinde 2 Temmuz 2018 tarihinde belediye oylamasını mobil uygulama üzerinde Ethereum ağı kullanmak üzere başarıyla tamamlamıştır [12].

2.6 Tayland'da Zcoin ile Demokrat Parti içi Başkan Seçimi

Zcoin blok zinciri üzerinde etkinlik için özelleştirilmiş bir mobil uygulama veya Rasberry PI üzerinde çalışan bir uygulama ile seçim bürosundan oy kullanabilen seçmenleriyle Tayland Demokrat Partisi, 1-9 Kasım 2018 tarihleri arasında yapılan seçimde parti başkanını seçmek için blok zinciri teknolojisini kullanan ilk siyasi parti olmuştur. Mobil uygulama üzerinden katılım gösteren seçmenlerin fotoğraflı kimlik gönderimi ile yetkilendirilmesi sağlanmıştır. Çevrimiçi oylama sisteminde, 120.000'den fazla parti üyesi katılım göstermiştir [13].

3. BLOK ZİNCİRİ

Son yıllarda popülerliğini daha da artırmış olan ve kendisinden sıkça bahsettiren bu teknoloji aslında veri yönetim kısaca veritabanı sistemidir. Verinin depolanma ve yönetim teknolojisi olan blok zinciri, verinin tutulduğu her bir bloğun zaman damgası ile kendinden önceki bloğun da özet bilgisini (hash) tutacak şekilde kronolojik olarak dijital imzayla birbirlerine eklenerek oluşturulmasıdır [14].

Blok zinciri üzerinde yeni bloğun oluşturulması ile sürekli büyüyen doğrusal yapıya bir sahiptir. Sağlıklı blok zincirinde son bloktan ilk bloğa kadar veriler doğrulanabilmektedir. Blok zincirinin güçlü yönlerinden birisi de dağıtık yapıda kullanılabilmesidir. Her bir zincir kopyası ağ üzerindeki diğer makinelerce tutulması anlamına gelmektedir. Dağıtık yapıda kurgulandığında ise, saldırı maliyetini artırarak oldukça zor hale getirmektedir. Çünkü verilerin değiştirilmesi için ağ üzerinde ele geçirilmiş çok sayıda makineye ihtiyaç vardır. Bu yüzden blok zinciri güvenilir olarak sistemler içerisinde yerini almıştır [15].

Blok zincir teknolojisi dağıtık yapısıyla birbirleri arasında güven sorunu teşkil eden taraflar arasında pahalı çözümler ihtiyacını ortadan kaldırarak ölçeklenebilir, esnek, verimli, şeffaf, hızlı çözüm aracı olarak alternatif hale gelmiştir.

3.1 Blok Zincirinin Tarihçesi

Blok zincirinin temeli; Stuart Haber ve W. Scott Stornetta tarafından dijital belgelerin zaman damgası ile değiştirilemeyen veya geçmişe yönelik belgelerin bütünlüğünü koruyacak şekilde 1991 patentli olarak tanımlanmıştır. 1992 yılında ise sisteme Merkle ağaçları yapısını tasarımla birleştirerek tek blok içerisinde birden fazla belgenin tutulmasını sağlamış ve sistem performansını iyileştirmiştir. Kullanılmayan bu teknolojinin patenti ise 2004 yılında son bulmuştur.

Stuart Haber ve W. Scott Stornetta'nın patentinin sona ermesi ile kriptografi aktivisti olan Hal Finney (Harold Thomas Finney II) 2004 yılında yeniden kullanılabilir iş ispatı olan RPoW adlı bir sistemi tanıtmıştır. Bu sistem, değiştirilemez ve özgün bir

Hashcash tabanlı iş ispatı tokenı alarak çalışmaya başlamış ve karşılığında kişiden kişiye aktarılabilen bir RSA imzalı token oluşturmuştur. Bu sistem içerisinde dünyanın herhangi bir yerinde gerçek zamanlı olarak güvenli sunucu üzerinde doğrulayabilmesini mümkün kılan imzalı tokenlar sayesinde çifte harcama sorununu gidermiştir. Böylece RPoW, kripto paraların ilkel hali olarak ve mihenk taşı olarak değerlendirilmektedir.

3.2 Kripto Paralar: Bitcoin ve Ethereum

Satoshi Nakamoto adlı yazarın "Bitcoin: A Peer-to-Peer Electronic Cash System" makalesi ile Ekim 2008 yılında Bitcoin tanıtılmıştır. Merkez bankaları ve hükümetlerden bağımsız, dağıtık yapıda olan, eşler arasında para alma, gönderme sistemidir [15]. Nakamoto makalede blok zinciri teknolojisini, verilerin ağdaki katılımcılar arasında doğrulanarak kaydedilip, katılımcılar arasında dağıtık yapıda olan bir veri yapısı olarak tanımlamıştır [4].

2013 yılında, bir programcı ve aynı zamanda Bitcoin Dergisi'nin kurucularından biri olan Vitalik Buterin tarafından Bitcoin'in merkezi olmayan uygulamalar geliştirebilmesi için betik bir dile ihtiyaç duyduğunu belirterek yeni bir kripto para sistemi geliştirmeye başlamıştır. Akıllı sözleşme olarak adlandırdığı kodlama işlevi olan yeni dağıtık tabanlı blok zinciri teknolojisi olarak Ethereum'u sunmuştur. Akıllı sözleşmeler Ethereum Blok Zincirinin üzerinde kaydedilen ve Ethereum Sanal Makinesi (EVM) üzerinde çalışan programlardır.

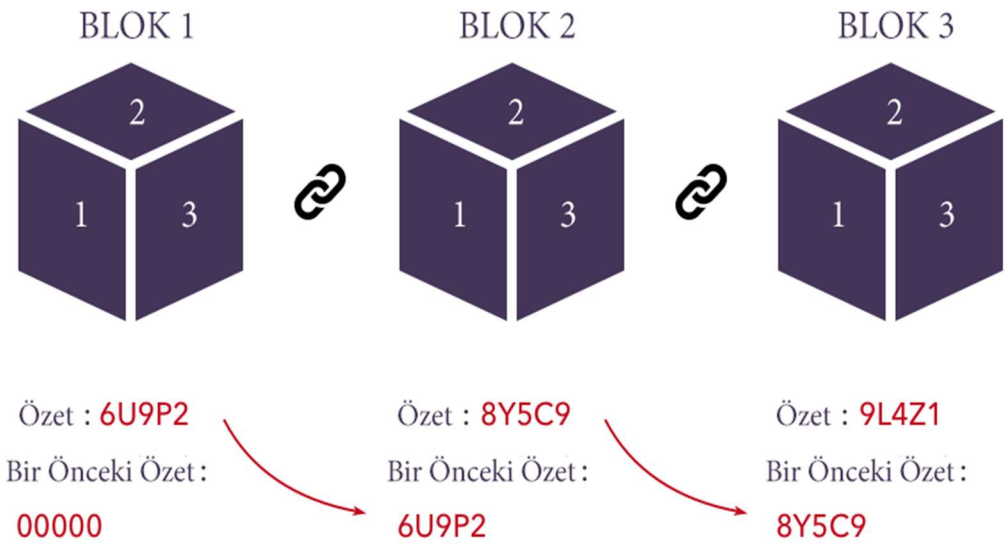
Kripto para blok zincirleri; herhangi bir aracı olmaksızın, düşük masraflarla özellikle tarafların arasında güvenin önem teşkil ettiği sektörlerde güvenilir altyapı sağlamaktadır. Emtia işlemleri, gayrimenkul alım-satım, lisans, doküman, patent, telif, noter kayıtları, kitlesel fonlama, tedarik, müşteri sadakat sistemleri, sağlık sektörü genelinde, kiralama hizmetleri, çevrimiçi oylama sistemleri, SWIFT ve benzeri bölgesel ödeme sistemleri gibi yüzlerce alandan sadece bazılarıdır.

3.3 Temel Blok Yapısı

Blok zincir; üzerinde her yeni veri bir önceki bloğun özet bilgisiyle tutularak oluşan yapı olarak adlandırılmaktadır.

Şekil 1'de gösterildiği üzere Bir blok 3 ana bölümden oluşmaktadır:

1. Bir öncesindeki bloğun özet (hash) bilgisi: Kendisinden önceki bloğun özet bilgisini tutarak kronolojik olarak verinin bütünlüğünü ve güvenliğini sağlayan bölümdür.
2. Bloğun barındırdığı veri: Blok içerisinde tutulan verinin içeriği yer almaktadır. Bu bölüm blok zinciri üzerindeki verilerin okunmasında kullanılmaktadır. İçerisinde herhangi bir veri barındırılabilmektedir.
3. Bloğun kendi özet (hash) bilgisi: Kendisinden sonraki eklenecek olan bloğun önceki özet (hash) bilgisi olarak yer almaktadır. Blok içerisinde veri ve önceki bloğun hash bilgisi ile üretilir, böylece zincir arasında verilerin üzerinde herhangi bir değişiklik olup olmayacağı anlaşılabilir. Çünkü manipüle edilmiş veri ile oluşturulacak özet bilgileri farklı olacağından zincir üzerinde kopmalara neden olacaktır.



Şekil 1: Blok zinciri yapısı

3.4 Blok Zinciri Nasıl Çalışır?

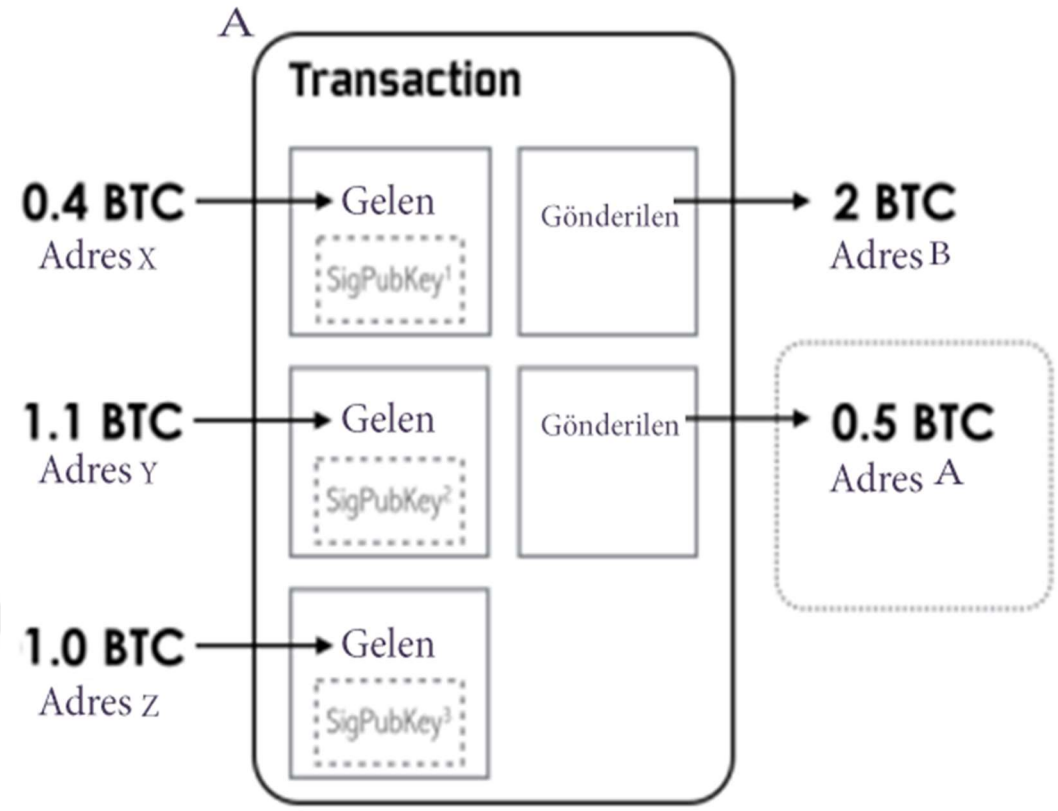
Blok zinciri nasıl çalışır sorusu, eşten eşe (peer-to-peer, P2P) aracısız kripto para transfer aracı olarak üzerinden açıklanabilir. Blok zincirinin çalışma prensibi 3 ana başlıkta toplanabilmektedir:

1. Transaction oluşturulması
2. Transaction'ın blok zinciri ağında onaylanması
3. Blok zincirine transaction'ın eklenmesi

3.4.1 Transaction oluşturulması

Gönderim-alım gibi işlemleri yapabilmek için bir kripto para cüzdanına sahip olmak gerekmektedir. Cüzdan içerisinde kişiye ait olan benzersiz açık ve gizli olmak üzere iki adres bulunmaktadır. Açık adres bilgisi ile kişiye gelecek olan transferlerde kullanılır. Gizli adres bilgisi ise kişinin başka bir hesaba gönderim yapmasında kullanılır.

Örneğin kripto para birimi olan Bitcoin transferi ile açıklamak gerekirse, A kişisi B kişine 2 Bitcoin göndermek istemektedir. İlk önce A, B'nin açık adresini biliyor olması yeterlidir. Blok zinciri ağında toplam bakiye bulunmamaktadır. Cüzdan gönderilmek istenen miktara ulaşana kadar blok zinciri üzerinde araştırma yapar. Şekil 2'de gösterildiği X, Y, Z cüzdanlarından A'ya gelen transferler ile B'ye gönderilmek istenen miktara ulaştığında cüzdan uygulaması arka planda bir transaction başlatılabilmektedir.



Şekil 2: Transaction yapısı

Transaction için Y ve Z (1.0 + 1.1) adreslerinden gelen miktar yeterli gibi görünse de blok zincirinin kronolojik (yeniden-eskiye) yapısı nedeniyle kayıtlar en yeni transferlerden eski transferlere doğru miktar tespiti yapılmaktadır.

Gönderilmek istenen miktar; 2 Bitcoin olsa da zira transaction için sistemin bulduğu 2.5 Bitcoin'dir. Bu durumda A'nın başlattığı transaction'da 2 Bitcoin B cüzdanına gönderilirken, kalan 0.5 Bitcoin ise A'nın cüzdanına yeni transferi olacak şekilde ayarlanır.

Transaction'ın tam anlamıyla başlatılabilmesi için son olarak bu işlemin gerçekten de A tarafından yapıldığının kanıtlaması gerekmektedir. Kanıt için A'nın cüzdanında yer alan gizli adresi ile transaction'ı kullanarak kriptografik bir dizi yöntem sayesinde dijital imza oluşturulur. Bu imza blok zinciri ağı üzerinde yer alan kişiler tarafından transaction'ı oluşturanın A olduğunu kanıtlamak için kullanılacaktır. Sonrasında transaction onaylanması için imza ile birlikte blok zinciri ağına gönderilir.

3.4.2 Transaction'ın blok zinciri ağında onaylanması

Blok zinciri ağı üzerinde yer alan kullanıcılar, transaction'ı blok zincirine eklemeden önce doğruluğunu kontrol ederler. Bu doğrulama için 2 aşamadan oluşmaktadır. İlk aşamada transaction içerisinde gönderilmek istenen A tarafından Bitcoin / Bitcoin'lerin daha önce kullanıp kullanılmadığını kontrol edilir. İkinci aşamada ise transaction içerisindeki imzanın doğru olup olmadığı kontrol edilir. Her iki aşamada kontrol edilip doğrulanırsa transaction blok zincirine eklenme aşamasına geçilir.

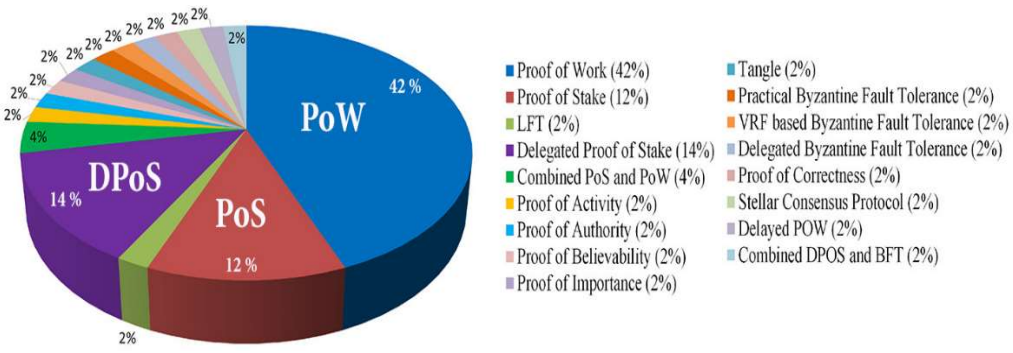
3.4.3 Blok zincirine transaction'ın eklenmesi

Blok zinciri ağı üzerinde doğrulaması yapılmış olan transaction havuzda kuyruğa alınır. Transaction'ların blok zinciri defterlerine yazılması ise blok zincircilerine fikir birliği algoritmaları ile olmaktadır. Kripto para biriminin teknolojisine blok zincirinde kullanılan algoritmaların çalışma prensipleri değişmektedir. Bu algoritmalar sayesinde transaction blok zincirine eklenir ve ardından tüm düğümler (node) arasında yayılması sağlanmaktadır.

3.5 Dağıtık Veri Yönetimi ve Fikir Birliği Algoritmaları

Geleneksel veri depolama sistemleri sunucular (server) üzerinde tutulmaktadır. Veriler sunucuda tek bir merkezi otoriteye bağlı tutulduğu için saldırıya açık durumdadır. Erişime yetkili olan kişi veya kişiler tarafından veriler kolayca manipüle edilebilir [16]. Blok zincirinin dağıtık yapıda kullanılıyor olması verilerin bütünlüğünü garanti altına almaktadır. Veriler üzerinde değişiklik yapılması ise ancak blok zinciri ağında yer alan makinelerin en az %51 çoğunluk ile eş zamanlı olarak ele geçirilmesi ile mümkün olmaktadır [17]. Teoride mümkün olsa da pratikte oldukça zordur.

Blok zinciri üzerinde verilerin düğümler arasında eş olarak kalabilmeleri için aralarında fikir birliği sağlanmalıdır. Bu durumun için düğümler arası fikir birliği algoritmaları ile sağlanmıştır. Temel blok yapısında bahsedilen, bir önceki bloğun özet (hash) bilgileri zaman damgalı olarak üretilir. Yeni eklenen bloğun önceki bloğun özet bilgisi ile eklenmesiyle zincirin devamlılığı sağlanmaktadır.



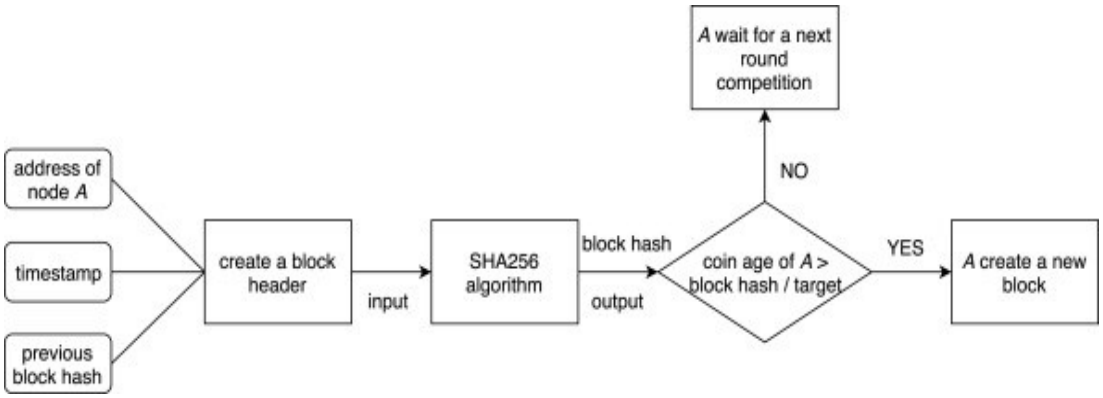
Şekil 3: Piyasa değerine göre 50 kripto para biriminin fikir birliği algoritmaları [18].

Fikir birliği algoritmaları kripto para birimlerinin teknolojilerine göre değişiklik gösterse de Şekil 3'te gösterildiği gibi %42 oranında iş ispatı (PoW), %12 oranında hisse ispatı (PoS) veya %14 oranında da yetkilendirilmiş hisse ispatı (DPoS) algoritmaları en yaygın olarak kullanılmaktadır [16].

3.5.1 İş İspatı (PoW)

İş kanıtı (PoW) fikri ilk olarak 1993 yılında Cynthia Dwork ve Moni Naor adlı bir makalede açıklanmıştır, ancak "iş kanıtı" olarak isimlendirilmesi ve literatüre dâhil edilmesi 1999 yılında Markus Jakobsson ve Ari Juels'in çalışmalarıyla olmuştur. İlk kullanımı olarak istenmeyen (spam) e-posta gönderenleri engellemek için kullanılmıştır [19].

İş ispati (PoW) Kripto para birimleri arasında ilk olarak Bitcoin ile kullanılmaya başlamıştır. Günümüzde birçok kripto para birimlerinin blok zinciri alt yapılarında oldukça popüler hale gelmiştir. Bu algoritmanın temel görevi blok zinciri ağının sürdürülebilirliği ve sürekliliğini sağlamaktır. Ağ üzerinde madenci ismi verilen ve blok zincirine yeni bloklar eklemekle görevli makineler yer almaktadır. Bu blokların eklenebilmesi ise bazı karmaşık matematik problemlerinin çözülmesiyle mümkün olabilmektedir. Problemleri çözmek hayli zor olduğu için güçlü işlem gücüne sahip donanımlara ihtiyaç duyulmaktadır. En fazla hesaplama gücünü elinde bulunduranlar en fazla kazananlar olmaktadır.



Şekil 4: İş ispatı (PoW) akışı

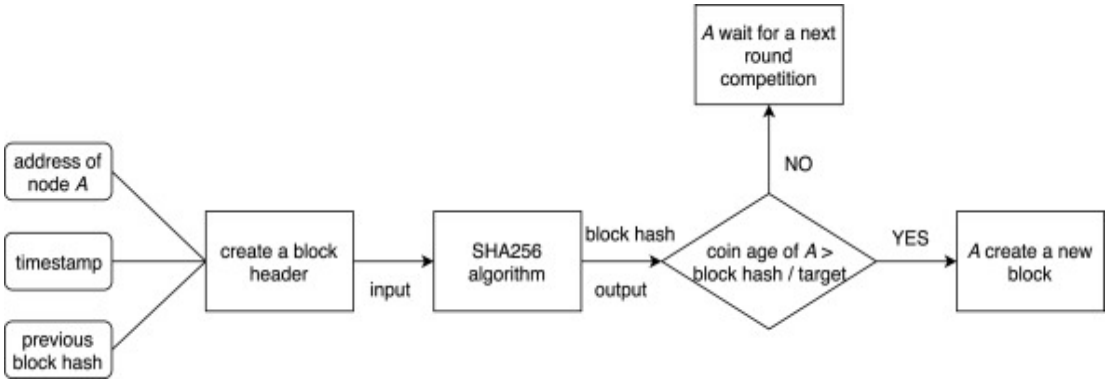
Problemi çözen ve bloktaki işlemleri doğrulayan ilk madenci işlemi ağa yayınlayarak ağda belirlenen kripto para ödülünü ve bloktaki işlemler için ödenen işlem komisyon ücretlerini almaya hak kazanır. Madenciler tarafından doğrulanan ağda yayınlanan işlemler blok zinciri sistemine kaydedilir.

3.5.2 Hisse ispatı (PoS)

Hisse ispatı (PoS) ilk olarak 2012'de Sunny King ve Scott Nadal tarafından bir makalede tanıtıldı ve Bitcoin madenciliğinin yüksek enerji tüketimi sorununu çözmeyi amaçlamıştır. Enerji tasarrufu sağlayan algoritmadır. Hesaplama gücü yerine sermaye gücüyle belirgin olarak ön plana yer almaktadır. Güçlü donanımları kullanarak işlemleri yapmak yerine fazlaca kripto paraya sahip olmak gerekmektedir [20]. Hesabında daha fazla kripto para tutan bir kullanıcı, ağdaki gücünü de arttırabilmektedir. Ağ üzerinde gücü kullanarak doğrulama işlemi için bazı kuralları esas almaktadır. Hesabında daha fazla kripto paraya sahip kullanıcıların doğrulayıcı olma ihtimali artmaktadır. PoS protokolü, cüzdan sahiplerinin yapılan işlemleri onaylayarak komisyonlardan gelir elde etmesine dayanmaktadır. Hesabında fazla kripto parası olan kullanıcı, gelirden daha fazla pay oranı almaktadır. Ancak gelir dağılımı PoS türlerine göre farklılık gösterebilir.

En çok kriptoya sahip kullanıcının ağda tekelleştirmesini engellemek için Hisse Kanıtı algoritması, blok tanımlamaları için birden fazla seçenek kullanır. En bilinen PoS seçim türleri, rastlantısal ve hesabındaki kripto paranın yaşına bağlı seçimdir. Rastlantısal seçim türünde işlemleri onaylayanlar, hesaplama gücü bakımından en zayıf ancak hisse (pay) değeri bakımından en varlıklı düğümler arasından

seçilmektedir. Kripto para yaşına bağlı seçimde ise, hesaplarındaki kriptoların yaşı olarak en uzun tutan kullanıcılar onaylayıcı seçilirler [20]. Doğrulamanın ardından her iki türdeki onaylayıcılar da işlem komisyonlardan gelir elde ederler.



Şekil 5: Hisse İspatı (PoS)

PoS algoritmasını ilk kullanan kripto para birimi PPcoin'dir. 2017 den sonra ortaya çıkan kripto para projeleri tarafından çoğunlukla tercih edilmiştir. Ethereum 2.0 güncellemesi ile PoW'dan PoS'a geçiş yapacak olması algoritmaya karşı ilgi ve güvenide artırmıştır [21].

3.5.3 Yetkilendirilmiş hisse ispatı (DPoS)

Yetkilendirilmiş Hisse İspatının DPoS'nin temel ilkesi, hisseye sahip düğümlerin blok doğrulayıcıları seçmesine izin vermektir [9]. Bu oylama yöntemi, paydaşların blokları kendileri oluşturmak yerine destekledikleri delegelere blok oluşturma hakkı vermelerini sağlar, böylece hesaplama güç tüketimini 0'a düşürür. DPoS akışını Şekil 6'da yer almaktadır. DPoS, bir Parlamenter sistem, Şekil 6'da gösterildiği gibi, delegeler sıralarında blok oluşturamazlarsa, görevden alınır ve paydaşlar bunların yerine yeni düğümler belirlerler. DPoS, adil ve demokratik bir şekilde bir fikir birliğine varmak için hissedarların oylarından en iyi şekilde yararlanır. PoW ve PoS ile karşılaştırıldığında DPoS, düşük maliyetli ve yüksek verimli bir konsensüs protokolüdür.

3.5.4 Popüler fikir birliği algoritmalarının karşılaştırılması

En iyi, en mükemmel fikir birliği algoritması yoktur. Her bir algoritmanın artıları ve eksileri bulunmaktadır. Tablo 1'de popüler olan fikir birliği algoritmalarının karşılaştırılması yer almaktadır.

Algoritma	Güvenlik	Saldırı Tolerasyonu	Kaynak Tüketimi	Onay Süresi	İşlem Hacmi	Çatallanma	Kripto Para
PoW	Yüksek	< % 25 Hesaplama Gücü	Yüksek	Uzun	Küçük	Kolay	Bitcoin [4]
PoS	Yüksek	< % 51 Hisse Gücü	Orta	Orta	Küçük	Kolay	Peercoin [21]
DPos	Normal	< 51 % onaylayan	Düşük	Kısa	Normal	Zor	Bitshares [24]

Tablo 1: Popüler fikir birliği algoritmalarının karşılaştırılması [22, 23].

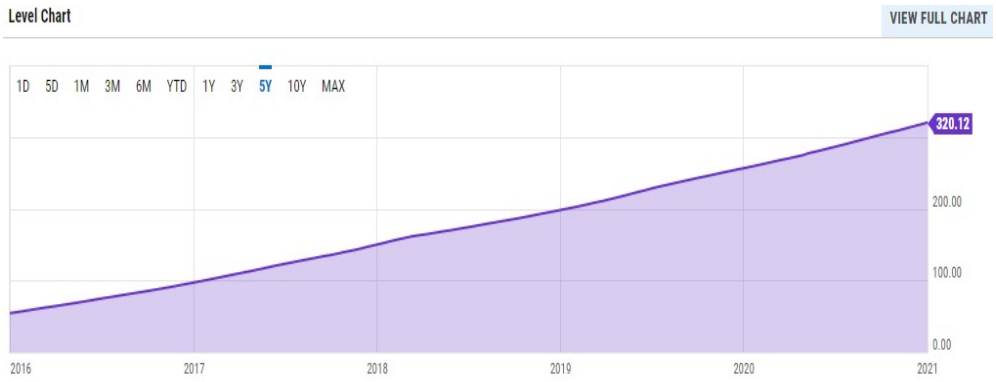
3.6 Blok Zinciri Ağ Türleri

Son yıllarda blok zincirinin farklı varyasyonları ortaya çıkmıştır. Genel (public), özel (private), ve konsorsiyum (B2B- işletmeler arası) olmak üzere 3 tip blok zincir ağı vardır.

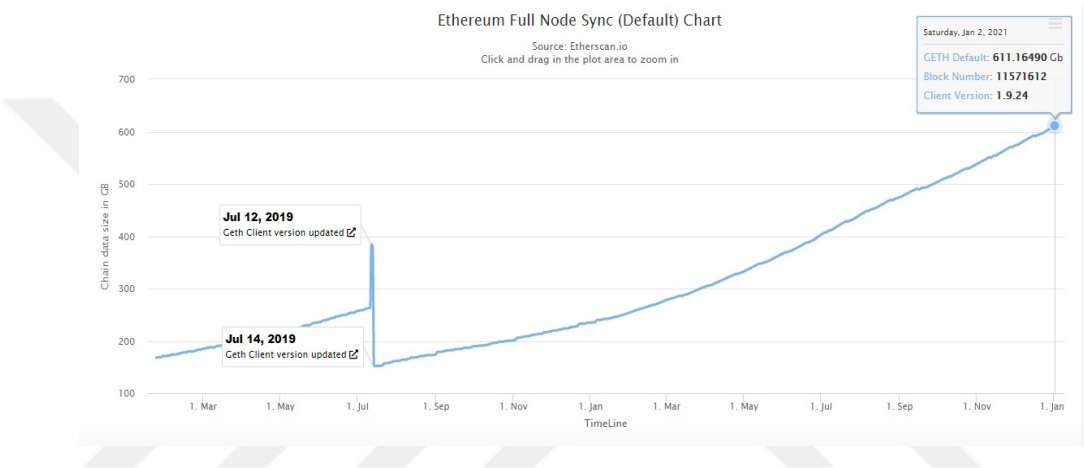
3.6.1 Genel blok zincir ağları

Genel blok zinciri ağdaki katılımcılar arasında erişim kısıtlaması bulunmayan ağlardır. İnternet bağlantısı olan herkes ağ üzerinde bir işlem gerçekleştirebilir. Ayrıca Genel blok zincirleri PoW/PoS fikir birliği algoritmaları ile katılımcıların kazanç sağlaması için ödüllendirme yapmaktadır. Çok fazla işlem gücü gerektiren donanımlara ihtiyaç duyması ve gizliliğin az olması zayıf yönlerinden sayılabilir.

En büyük ve en bilinen genel blok zincirleri Bitcoin ve Ethereum'dur ve defter boyutları her geçen gün artmaktadır. Şekil 6'da Bitcoin Blok Zinciri'nın boyunun 320 GB [25] ve Şekil 7'de Ethereum 611 GB [26]'ı geçtiği gösterilmektir.



Şekil 6: Bitcoin Blok Zinciri Boyutu [25], 02.01.2020.



Şekil 7: Ethereum Blok Zincir Boyutu [26], 02.01.2020.

3.6.2 Özel blok zincir ağları

Genel blok zincirine benzer olarak dağıtık yapıda olan, eşler arası (P2P peer-to-peer) blok zinciri ağıdır. Bu ağın yönetimi tek bir kuruluşa aittir. Bu kuruluş ağa kimlerin katılacağına, fikir birliği algoritmaları ile kimlerin kaydedici veya onaylayıcı yetkilerine sahip olduğunu kontrol eder. Kullanım uyarlamasına bağlı olarak katılımcılar arasında güven mekanizmasını sağlamaktadır. Özel blok zinciri ağına örnek olarak Hyperledger ve kripto para birimi olan Ripple verilebilir.

3.6.3 Konsorsiyum blok zincir ağları

Konsorsiyum blok zincir ağlar işletmeler arasında çalışmaktadır. Kuruluşlar tarafından ağ katılımcılarının hangi işlemleri yapabileceği, görüntüleyebileceği veya erişim kısıtlamaları özel blok zinciri ağlarındaki gibi izinlerle olmaktadır. Bu ağlara örnek olarak Quorum ve Corda blok zincirleri yer almaktadır.

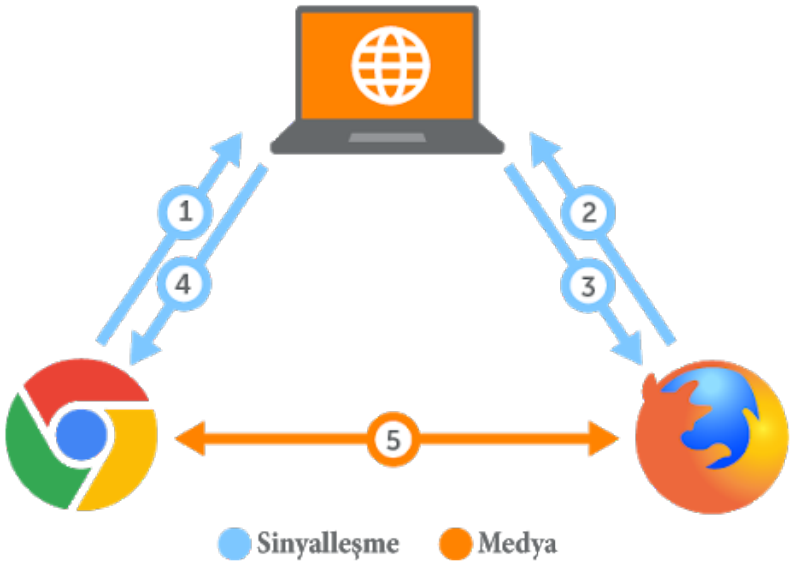
4. WEBRTC

2011 yılında Google tarafından tanıtılan WebRTC eşler arasında (P2P, peer-to-peer) olarak ses, görüntü ve veri aktarımını gerçek zamanlı olarak herhangi bir medya sunucusuna ihtiyaç duymadan yapabilmektedir [27]. WebRTC kullanılması ücretsiz, açık kaynak kodlu bir teknolojidir. Google, Apple, Mozilla, Microsoft ve Opera tarafından desteklenmektedir. Şekil 8'de gösteriliği üzere web ve mobil platformlarda olmak üzere modern tarayıcılar tarafından desteklenmektedir [28].

Şekil 8: Modern tarayıcılarda WebRTC desteği [28].

WebRTC standardizasyonu için Internet Engineering Task Force (IETF) ve World Wide Web Consortium (W3C) tarafından desteklenmektedir.

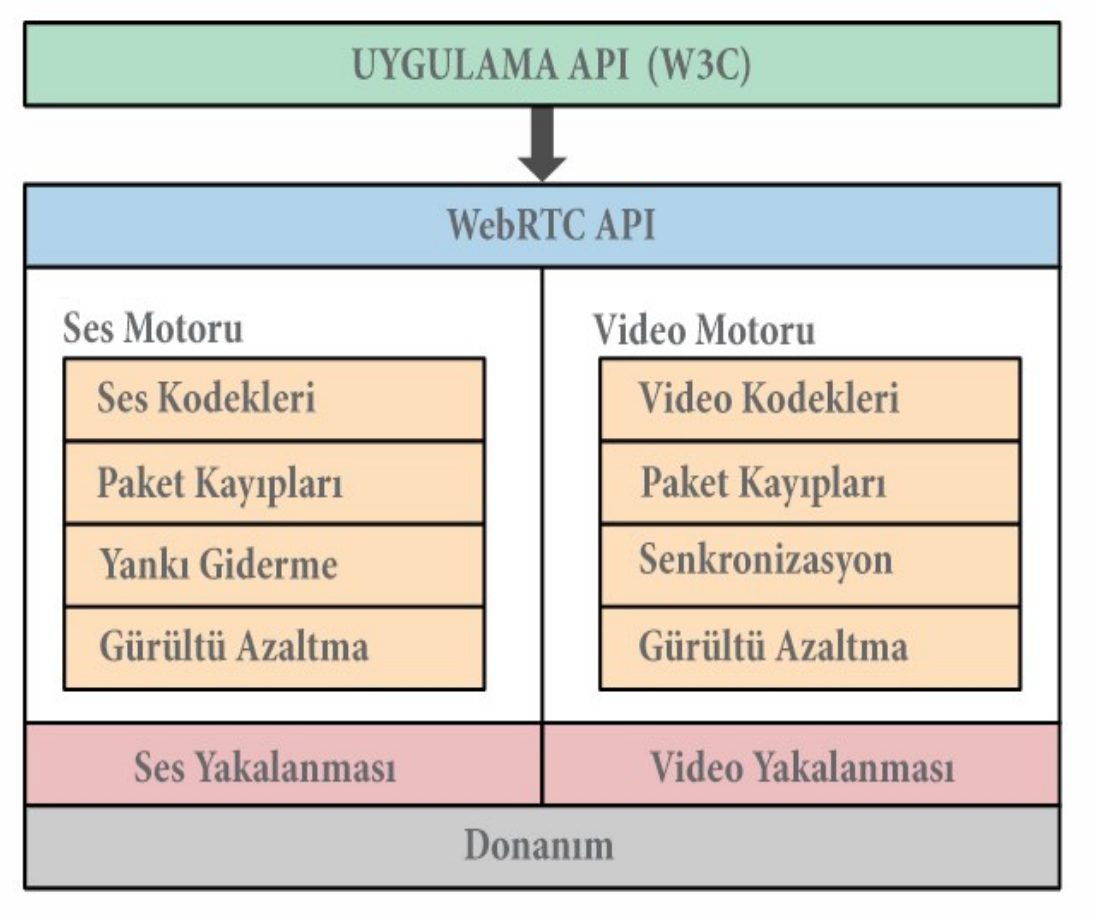
WebRTC tarayıcı üzerinde herhangi bir eklenti kurmadan ses, görüntü ve veri aktarımları yapabilen zengin içeriklere sahip, gerçek zamanlı web uygulamaları geliştirmek için alt yapı sunmaktadır. HTML5 ve JS kullanılarak tarayıcı üzerinde çalışan performanslı uygulamalar hızlı geliştirilebilir. Günümüzde popüler uygulamalardan başlıca Googel Meet, Google Hangouts, Facebook Messenger, Discord, Amazon Chime, Houseparty, Appear.In, Gotomeeting, Slack ve Whatsapp WebRTC teknolojisini kullanmaktadır.



Şekil 9: WebRTC temel prensibi

Geleneksel istemci-sunucu arası haberleşme üzerinde istemci her zaman sunucu üzerinden yanıt beklemektedir. Web soketlerinde istemci sunucu ile haberleşir ardından ilgili haberleşme sunucu üzerinden diğer istemcilere yayılarak gerçekleşmektedir. WebRTC'de ise bu durum farklıdır. Şekil 9'da gösterildiği üzere istemci haberleşmek istediği diğer istemcinin IP adresini sunucuya üzerinden sinyalleşme (signaling) HTTPS veya web soket bağlantısıyla öğrenir. İstemciler birbirlerinin adreslerini öğrendikten sonra kendi aralarında eşten eşe bağlantı ile medya akışı başlamaktadır [29]. WebRTC ile web tarafında uygulama geliştirmek için JS API'leri kullanılmaktadır. Aynı geliştirme mobil platformlarda yapılmak istenirse mobil işletim sistemlerine uygun kütüphaneler mevcuttur.

Tarayıcıda üzerinde kaliteli, verimli bağlantı sağlanabilmek adına WebRTC kendi içerisinde ses ve video motorlarına sahiptir. Şekil 10'da gösterildiği gibi bu motorlar sayesinde ses ve görüntü donanımlarını yakalar ve en kaliteli hale getirmek için yankı ve gürültü önleyici algoritmalar çalıştırmaktadır.



Şekil 10: WebRTC üzerinde ses ve video motorları

Girişten alınan ses içerisinde gürültü azaltma, yankı giderme işlemleri otomatik olarak ses kodekleriyle yapılmaktadır. Tüm işlem doğrudan tarayıcı içerisinde ses ve video motorları tarafından yapılır ve daha da önemlisi, tarayıcı, ses ve video akışlarının ve ağ oluşturma koşullarının sürekli değişen parametrelerini hesaba katmak için işlem hattını dinamik olarak ayarlanır. Dinamik optimizasyon sonunda işlenmiş olan içerik alınır veya uzaktaki istemciye API'ler üzerinden gönderilmektedir [30].

4.1 WebRTC API

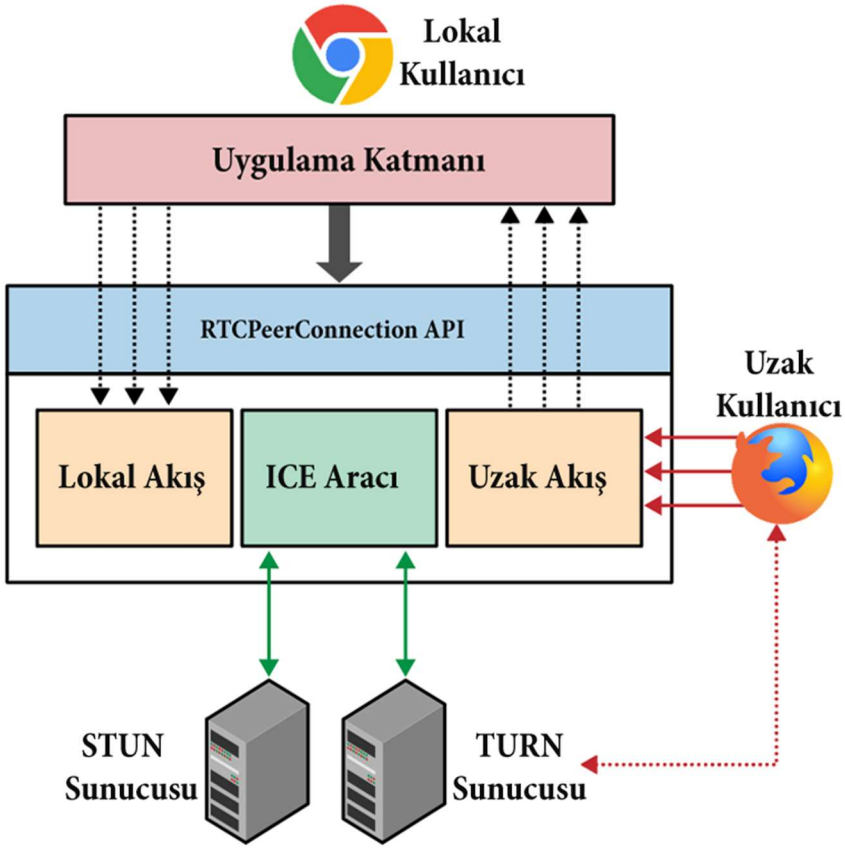
Eşler arasında ses, görüntü veya veri iletişimi gerçek zamanlı yapabilmek için WebRTC, JS tabanlı aşağıdaki API'leri sunmaktadır.

1. **RTCPeerConnection:** Eşler arası bağlantıyı kurmak ve kontrol etmek için kullanılır. Kullanıcılar arasında veri akışını güvenli hale getirmektedir.
2. **MediaStream:** Mikrofon, kamera gibi medya donanımlar erişmek için kullanılır.

3. **RTCDataChannel:** Eşler arasında paylaşılacak olan verilerin gönderileceği kanal sağlanır ve gönderimler web soket yapısına benzer olsa da veri direk iletişimde olunan istemciye gönderilir.

4.1.1 API: RTCPeerConnection

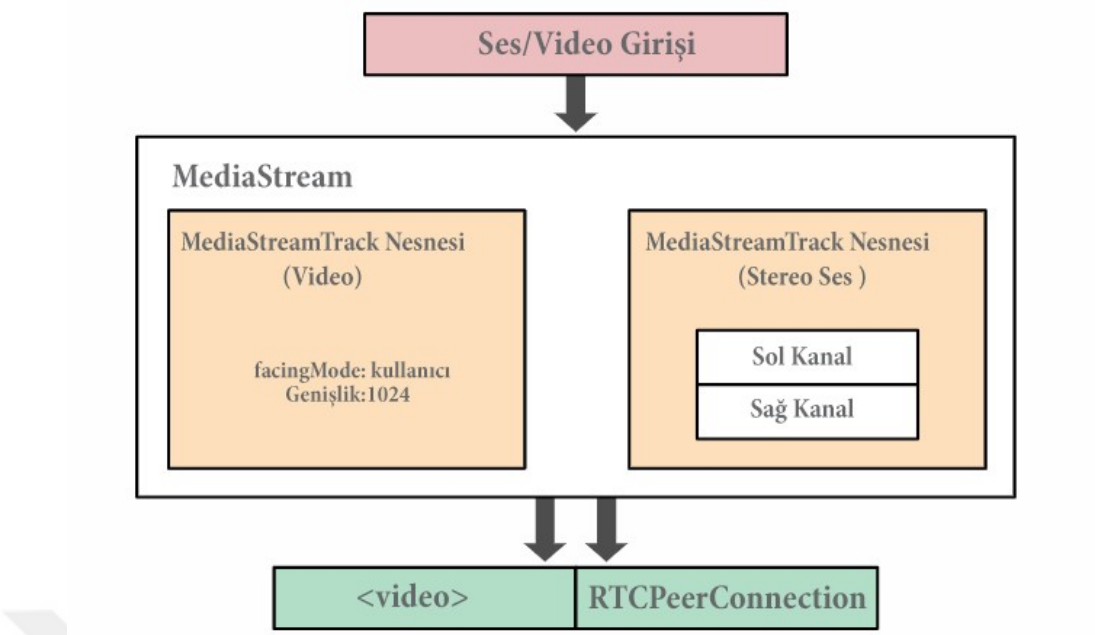
Şekil 11'de gösterildiği gibi uygulamanın temelinde yer alır ve eşler arası bağlantıların kurulması, veri akışının yönetilmesi, eşlerin durum bilgisi gibi tüm yaşam döngüsü bu protokol tarafından sağlanmaktadır [30].



Şekil 11: RTCPeerConnection yapısı

4.1.2 API: MediaStream

Şekil 12'de gösterildiği gibi medya içeriklerine erişimi HTML5 sayesinde destekleyen protokoldür. Kamera, mikrofon, giriş arabirimlerinden herhangi bir içerik, sabit disk sürücülerinden veya uzak ağ üstünden veri akışı sağlayabilmektedir.



Şekil 12: MediaStream yapısı

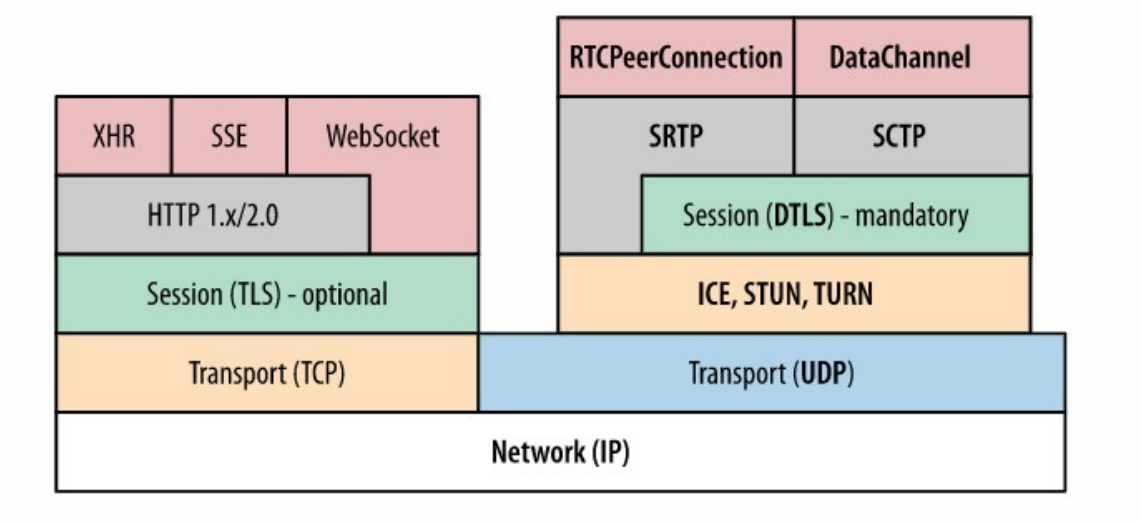
MediaStream nesnesi, gerçek zamanlı bir medya akışını temsil eder ve uygulama kodunun verileri almasına, tek tek parçaları işlemesine ve çıktıları belirlemesine olanak tanır. Gürültü giderme, eşitleme, görüntü geliştirme ve daha fazlası gibi tüm ses ve video işleme, ses ve video motorları tarafından arka planda otomatik olarak gerçekleştirilir [30, 31].

4.1.3 API: RTCDataChannel

Bu protokol sayesinde eşler arasında veri gönderimi yapılabilmektedir. Veri kanalları güvenilir veya güvenilmez olacak şekilde yapılandırılabilir. Güvenilmez olarak ayarlandığında, mesajlar otomatik olarak istemcilere tekrar gönderimi yapılmamaktadır. Ayrıca verileri iletme şekillerinde sıralı veya sırasız olarak yapılandırılabilirler. Mesajlaşma uygulamalarında sıralı iletim kullanılmakta olup, zaman aşımı süresi veya maksimum tekrar gönderim limiti koyularak veri gönderimi kısmen güvenilir olarak yapılandırabilir [30].

4.2 WebRTC'de Ağ Kullanımı

WebRTC gerçek zamanlı iletişimde ses, görüntü ve veri taşıması yapabilmek için Şekil 13'te gösterilen protokolleri kullanmaktadır. [30]



Şekil 13: WebRTC protokollleri

Güvenilirlik yerine zamanında olma gerekliliği, UDP protokolünün gerçek zamanlı verilerin teslimi için tercih edilen bir aktarım olmasının başlıca nedenidir. TCP, güvenilir, sıralı bir veri akışı sağlar: bir ara paket kaybolursa, TCP ondan sonraki tüm paketleri arabelleğe alır, yeniden iletimi bekler ve ardından akışı uygulamaya teslim eder. UDP, verilerin güvenilirliği veya sırası konusunda hiçbir vaatte bulunmaz ve her paketi geldiği anda uygulamaya teslim eder. Gerçekte, ağ yığınlarımızın IP katmanı tarafından sunulan en iyi çaba teslim modelinin etrafındaki ince bir paketleyicidir [30].

UDP, tarayıcıda gerçek zamanlı iletişimin temelidir ve UDP üzerinden eşler arası bağlantı kurmak ve sürdürmek için ICE, STUN ve TURN gereklidir. DTLS, eşler arasındaki tüm veri aktarımlarının güvenliğini sağlamak için kullanılır; şifreleme, WebRTC'nin zorunlu bir özelliğidir. SCTP ve SRTP, farklı akışları çoğaltmak, tıkanıklık ve akış kontrolü sağlamak ve UDP'ye ek olarak kısmen güvenilir teslimat ve diğer ek hizmetleri sağlamak için kullanılan uygulama protokolleridir [30].

4.2.1 Sinyalleşme ve oturum tanımlama protokolü (SDP)

Sinyalleşme, WebRTC teknolojisinin en önemli kısmındır. Sinyalleşme sürecinde kiminle nasıl bağlantı kurulacağı ve bağlantının hangi protokollerle sağlanacağının belirlenmesi işlevi olarak ifade edilebilir. Eşler arasında medya akışının başlatılabilmesi için bağlantı yapılacak olan eşlerin birbirlerini bilmesi aşamasına WebRTC içerisinde sinyalleşme adı verilmektedir. Şekil 10'da gösterildiği üzere WebRTC içerisinde iki eş HTTP el sıkışma mekanizması (XHR, SSE, WebSoket) ile

sinyalleşme sürecinde eşler birbirlerinin IP adresini öğrenerek medya akışına hazır olarak sinyalleşme süreci tamamlanır. Bu süreç medya akışı süresince dinamik olarak sürekli kontrol edilmektedir.

WebRTC, eşler arası bağlantının bilgilerini tanımlayabilmek için SDP kullanmaktadır. SDP bağlantının özelliklerini içeren bilgilerin tanımlanması için kullanılır. Bu bağlantı özellikleri şu şekildedir: kurulacak olan bağlantıdaki veri türü (ses, video, veri), IP adresleri, kodek bileşenleri, bant genişliği ve diğer meta veriler [30].

Sinyalleşme akışı aşağıdaki gibi anlatılabilir:

1. Teklif paketi içerisinde A'nın bağlantıyı açarak, uygulama katmanına geri dönecek bilgi ile karşı tarafın vereceği bilgiyi içeren SDP paketi oluşturulur ve SDP'yi sinyal sunucusuna iletilir.
2. Sinyalleşme sunucusu, A tarafından hazırlanan SDP paketini B'ye aktarır.
3. B Teklif paketini alır ve ip adresi bilgisini paket içerisine koyarak SDP sunucusuna geri gönderir.
4. B'nin sinyalleşme sunucusu A'ya SDP paketini geri gönderir.
5. A gelen paketi açarak B'nin iletişim adresini öğrenmiş olur, böylece aralarında medya akışı yapılabilecek eşler arası (P2P) bağlantı sağlanmış olur.

4.2.2 Etkileşimli bağlantı kurulumu (ICE)

Eşler arası bağlantı kurulması ve birbirlerine paket iletimlerinin yapılması gerekmektedir. Eşler arasında güvenlik duvarının olmadığı durumlarda basitçe birbirleri arasında bağlantı işletim sisteminin sağladığı IP adresi üzerinden kolayca yapabilmektedirler. WebRTC içerisinde sistem her zaman en kolay iletişim yolunu aramaktadır. IP adresi ile direkt olarak bağlantı sağlanamaz ise STUN TURN çözümleri eşler arasın bağlantı kurulabilir.

Kullanıcıların NAT arkasında olduğu durumlarda ise NAT sunucuları üzerinde STUN programlarını bu sorunu çözmek için kullanır. Genel IP adresini bulabilmek için STUN ile iletişime geçerek aldığı IP adresleri üzerinden bağlantı sağlanır. Kullanıcılar NAT arkasında olsa bile en önemli nokta medya akışı kendi aralarında gerçekleşir.

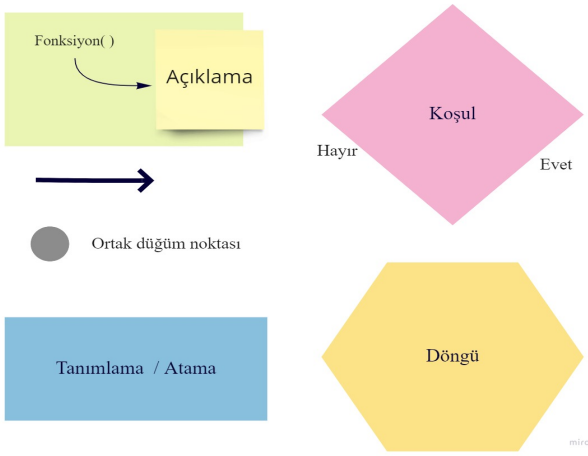
5. BLOK ZİNCİRİ TABANLI WEBRTC İLE GERÇEK ZAMANLI OYLAMA SİSTEMİ ÖNERİSİ

Seçimler demokratik sistemin gereğidir ve kavramsal olarak bir görevi icra edecek kişi, kişiler veya kurulun, ilgili alandaki katılımcı veya seçmenlerin vasıtası ile birçok aday arasından tayin edilmesidir [32]. Başka bir ifade ile yönetilenlerin kendi yöneticilerini belirleme işlemdir.

Seçimlerde yer alan ve ilgili alanda yöneticilerini seçme hakkına sahip olanlara seçmen, seçim haklarını kullanmalarına ise oy denilmektedir. Adil bir seçim ortamı yapılabilmesi için yeterlilik ve doğrulama, güvenilirlik, bütünlük, şeffaflık ve denetime açıklık, gizliliğin korunması ve baskı altına alınabilmesinin önlenmesi, esneklik, kolaylık, onaylanabilme ve uygun maliyet gibi ölçütlere de sahip olması gerekmektedir.

Seçim, seçmen ve oy kullanım hakkı kavramlarına uygun olarak bu bölümde çevrimiçi oylama sistemini blok zinciri tabanlı WebRTC ile gerçek zamanlı olarak sistemsel tasarım çalışmasına yer verilmiştir. Tasarım çalışmasında çevrimiçi sistemlerine uygun olarak web ve mobil platformları iç içe kullanarak akış şemaları hazırlanılmıştır.

Şekil 14'te belirtilen şekiller ile çevrimiçi oylama sistem önerisi teorik olarak açıklanmıştır.



Şekil 14: Akış şemasında yer alan şekillerin tanımlamaları

Yeşil alan: Akış içerisinde yer alan bu gösterim uygulama içerisinde kullanılacak fonksiyonların gösterimidir. Fonksiyon ismi yapacağı işlemlerin özetidir.

Kırmızı alan: Akış içerisinde temel koşul gösterimleri kırmızı olarak belirtilmiştir. Koşullar iki çıkışı olan mekanizmalardır, evet-hayır, doğru-yanlış, 1-0 gibi.

Gri daire alanı: Akış içerisinde fonksiyon, koşul veya döngülerin ortak bir düğüm noktasında buluşarak ortak bir akışta girme gösterimidir.

Mavi alan: Akış içerisinde bu alanda yaşam döngüsü içerisinde kullanılacak olan tanımlamaların yapıldığının gösterimidir.

Sarı alan: Akış içerisinde bu alanda tekrarlı işlemlerin gösterildiği döngüler gibi ardışık işlemlerin gösterimidir.

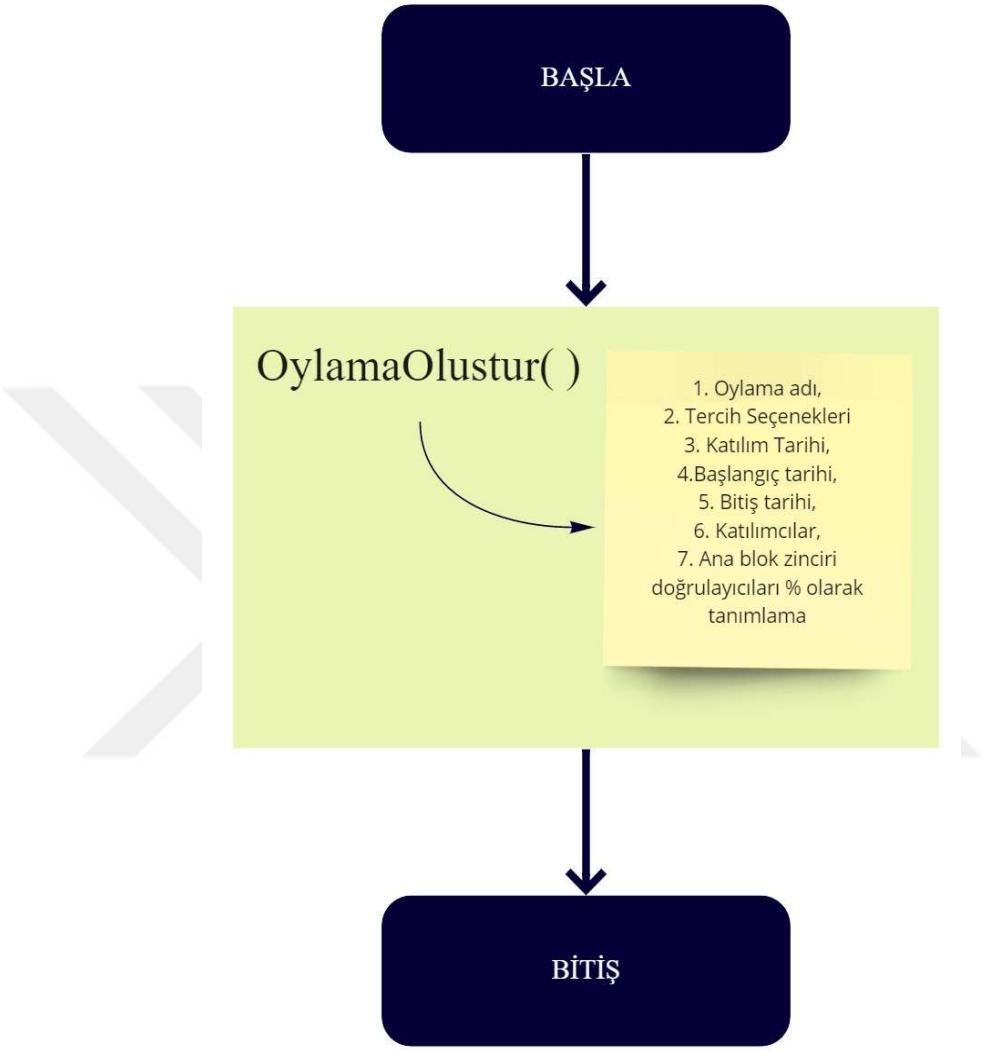
Oklar: Akış içerisinde fonksiyonlar, döngüler, koşullar arasında oluşan uygulama yönünü belirleyen gösterimdir.

5.1 Uygulama Akış Şemaları

Oylama etkinliği oluşturma, kullanıcının uygulama üzerinde yetkilendirilmesi, seçim süresince açılacak sandıkların dinamik olarak belirlenmesi, açılan sandıklara kullanıcıların atanması, oylama sürecinin başlaması, eşler arası mutabakatın sağlanması, ana zincir mutabakatı olarak 7 süreç akış tasarımı yer almaktadır.

5.1.1 Oylama etkinliği oluşturma

Şekil 15'te gösterildiği üzere web platformu üzerinde ilgili yetkililer tarafından oylama etkinliği şeması gösterilmiştir.



Şekil 15: Oylama başlatma akışı

Oylama oluştur fonksiyonu ile oylama temel bilgileri oluşturulur:

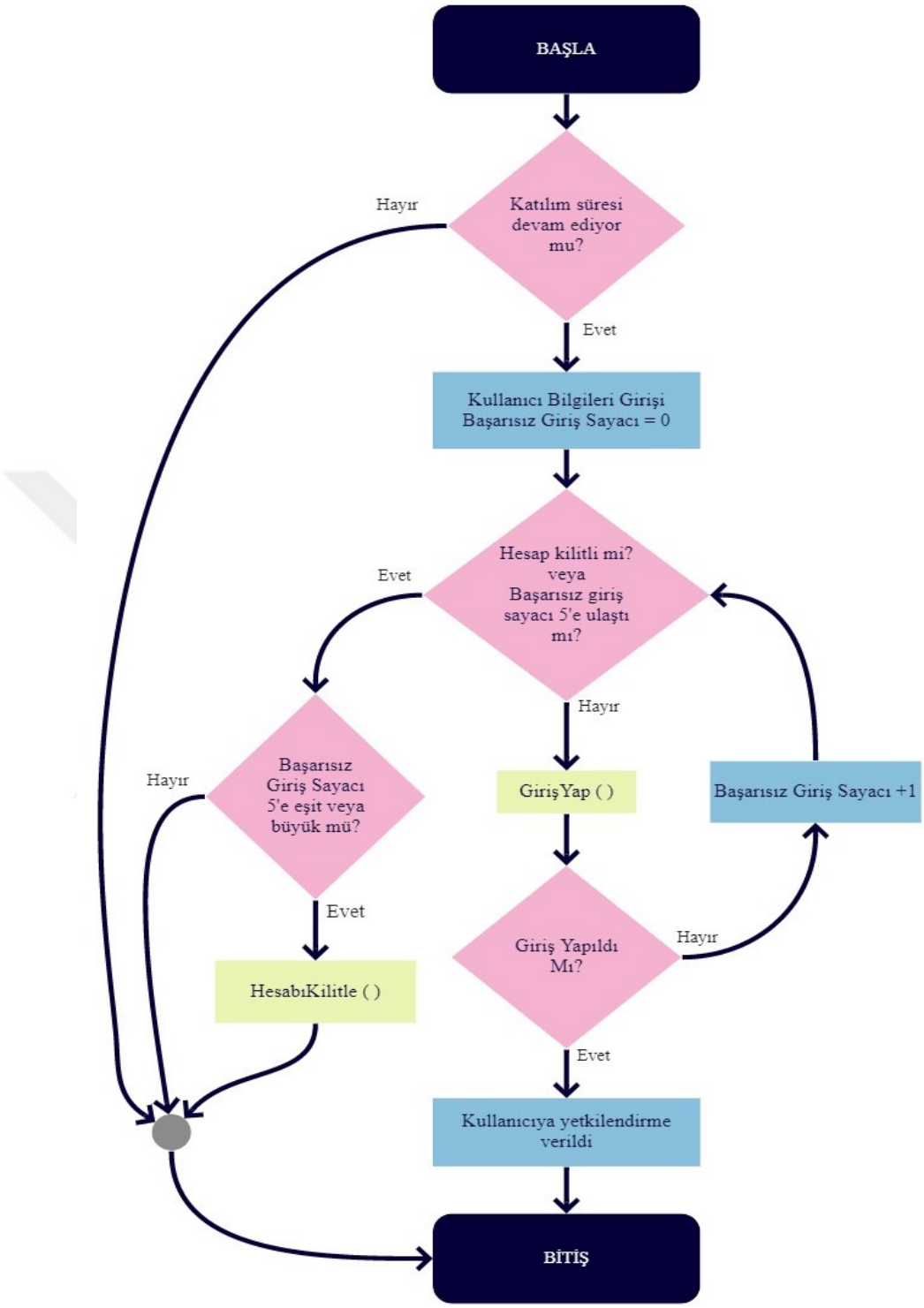
1. **Oylama Adı:** Oylamayı temel düzeyde tanımlayan alandır.
2. **Tercihler:** Seçmenlerin tercihlerini yapacağı seçeneklerin önceden belirlenmesidir.
3. **Katılım Tarihi:** Katılımcıların oylama sistemlerine dâhil olabilecekleri tarihtir. Bu tarihten başlangıç tarihine kadar sisteme giriş yapmaları gerekmektedir. Bu tarih

kısıtlaması dinamik olarak açılacak olan sandıkların sayısının belirlenmesinde kullanılacaktır.

4. **Başlangıç Tarihi:** Katılımcıların oy kullanım hakkının başlayacağı tarihtir. Bu tarih kısıtlamaları eşler arasında dağıtık yapı kurgulanması için önemli yere sahiptir.
5. **Bitiş Tarihi:** Bütün sandıklarda etkinliklerin tamamlanması veya bitiş tarihinin son bulması ile oylama süreci sona erip etkinlikler durdurulur.
6. **Katılımcılar:** Oylama sürecine dâhil edilecek ilgili katılımcıların oluşturulması.
7. **Ana Blok Zincir Doğrulayıcı Yüzdesi:** Oylama sürecinin sonunda sandık sonuçlarının doğruluğunu sağlayacak olan rastgele katılımcı oranı. Bu oran ile sandıkların oluşturulmasından sonra nihai katılımcılar arasından rastgele olarak bazı katılımcıların ana zincir doğrulayıcı olarak belirlenmelerini sağlar.

Akış şemasında temel olarak oylama sürecinin ilk basamağı olan etkinlik oluşturulma süreci tasarlanmıştır. Oylama ihtiyacına göre bilgiler girilirken farklı içerikler oluşturulması gerekebilir.

5.1.2 Kullanıcı yetkilendirilmesi giriş yapma süreci



Şekil 16: Katılımcının giriş yaparak yetkilendirilmesi

Şekil 16'da gösterilen akış şemasında bir kullanıcının oy kullanabilmesi için giriş yapma yani yetkilendirilmesi aşamaları yer almaktadır.

Bu aşama oy kullanım hakkı için gerekli bir aşamadır. Yetkisi olan kişilerce yapılması gerekmektedir. Bu yetkilendirme en basitinden kullanıcı bilgisi, parolası şeklinde yapılabilir.

İlk adımdaki koşul "Katılım süresi devam ediyor mu?" yetkili kişilerce belirlenen oy katılım tarihi kontrol etmektedir. Katılım tarih kontrolü uygun aralıkta değil ise kullanıcının yetkilendirilme süreci sonlandırılır. Katılımcı yalnızca uygun tarih aralığında kaydını tamamlayabilir. İlk koşulun önemi tarihlere uygun olarak yetkilendirme almış olan kullanıcılar arasında dinamik olarak sandıkların oluşturulabilmesi için önemlidir.

İlk koşulun sağlanması durumunda kullanıcı bilgileri alınır ve sisteme giriş denemesi sayacı tanımlanır. İkinci koşulda "Hesap kilitli mi veya Başarısız giriş sayısı 5'e ulaştı mı?" doğru ile yetkilendirilme süreci sonlandırma akışına sokulur. Bu akışta yer alan "Başarısız giriş sayısı 5'e eşit veya büyük mü?" sorusu ile hesabın kilitlenmesi sağlanır.

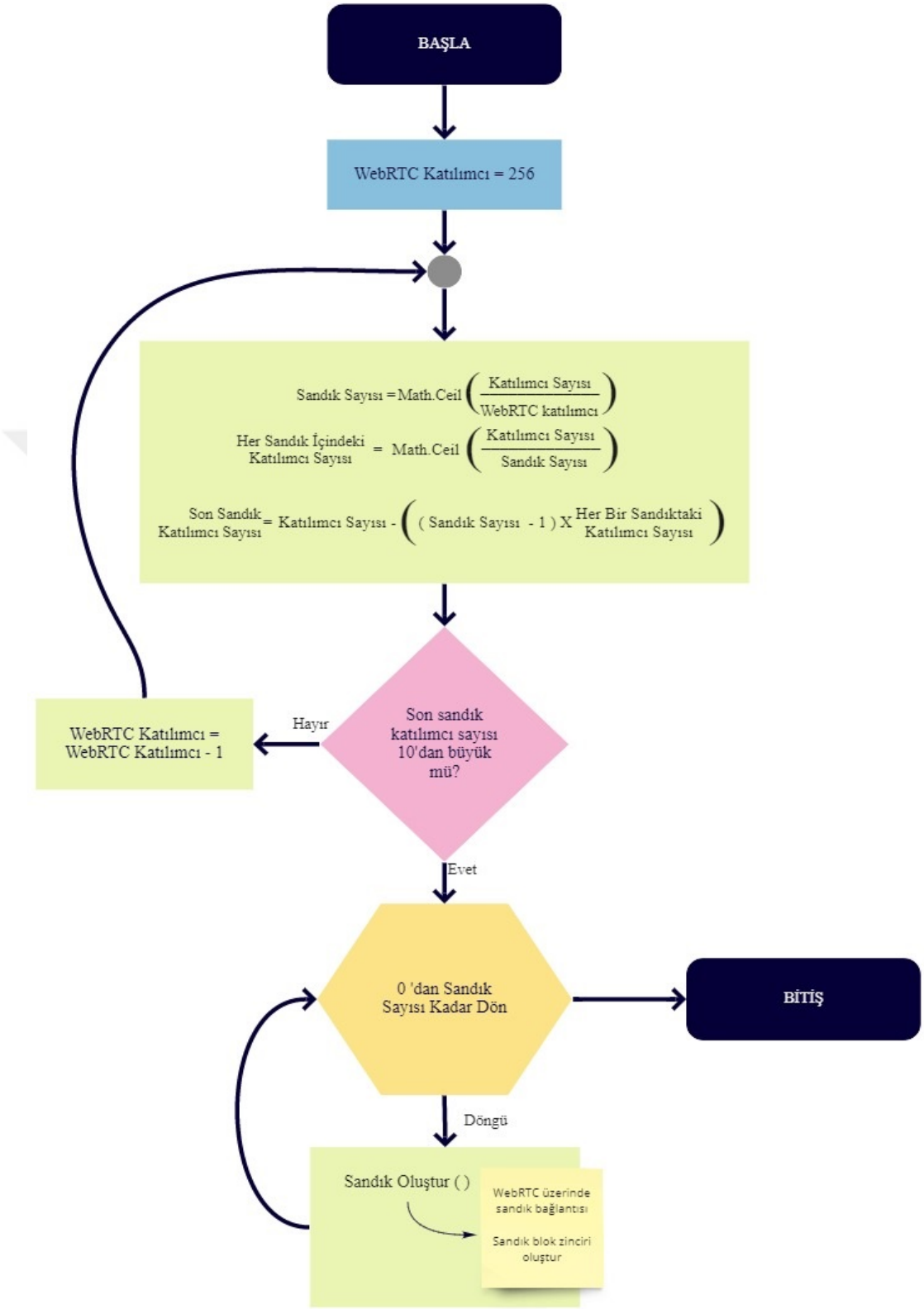
İkinci koşulun sağlanması ve başarısız giriş denemesi 5'e ulaşması durumunda hesabını kilitlenerek yetkilendirme süreci sonlandırılır.

Hesap kilitli değil, başarısız deneme sayısı da 5'ten küçük ise kullanıcının giriş bilgileri ile "Giriş Yap( )" fonksiyonu çağırılır.

Üçüncü koşul olan "Giriş yapıldı mı?" sorusu ile akış devam eder. Koşul doğru ise "Yetkilendirme verilir", yanlış ise başarısız giriş denemesi 1 artırılarak ikinci koşula kullanıcı yönlendirilir. Bu yönlendirme işlemleri kullanıcı başarısız giriş sayısını 5 oluncaya kadar veya başarılı işlem yapana kadar tekrar edilir.

Hesapların kilitlenmesi ile bazı güvenlik ihlallerinin önüne geçmiş olunur. Ekstra önlemler ile bu süreçlerin yönetilebilir. E-posta, SMS veya çeşitli kimlik doğrulamalar ile farklı güvenlik önlemleri kurgulanabilir.

5.1.3 Oylama sandıkların belirlenmesi



Şekil 17: Yetkilendirme almış katılımcılardan sandıkların oluşturulması

Şekil 17'de gösterilen akış şemasında katılım tarihinin bitmesi ve oylama sürecinin başlaması ile bir kullanıcıların katılacakları sandıkların oluşturma aşamaları yer almaktadır.

WebRTC altyapısı gereği en fazla 256 katılımcıya destek vermektedir [33]. Güvenlik açısından oluşturulacak alt zincir katılımcıların sayısı azami şekilde dağıtılması gerekir.

İlgili yetkilinin oluşturduğu oylama sisteminde katılımcıların önceden belirlenmesi gerekir. Oylama sisteminde bir oy etkinliğinin tekilliği oy kullanım ölçütlerine göre gereklidir [5]. Sandıkların belirlenmesinde katılımcısı sayısı ile her bir sandıkta bulunacak olan maksimum katılımcı sayısı göz önünde bulundurularak yapılmalıdır.

Sandık sayısı her bir sandıkta maksimum kullanıcı sayısı 256 olacak şekilde belirlenir. Burada önemli olan ölçüt açılacak olan sandık sayısı ondalık değerlere sahip olması ihtimal dâhilindedir. Bu durumda hesaplanan sandık sayısının yukarı yuvarlanması gerekmektedir.

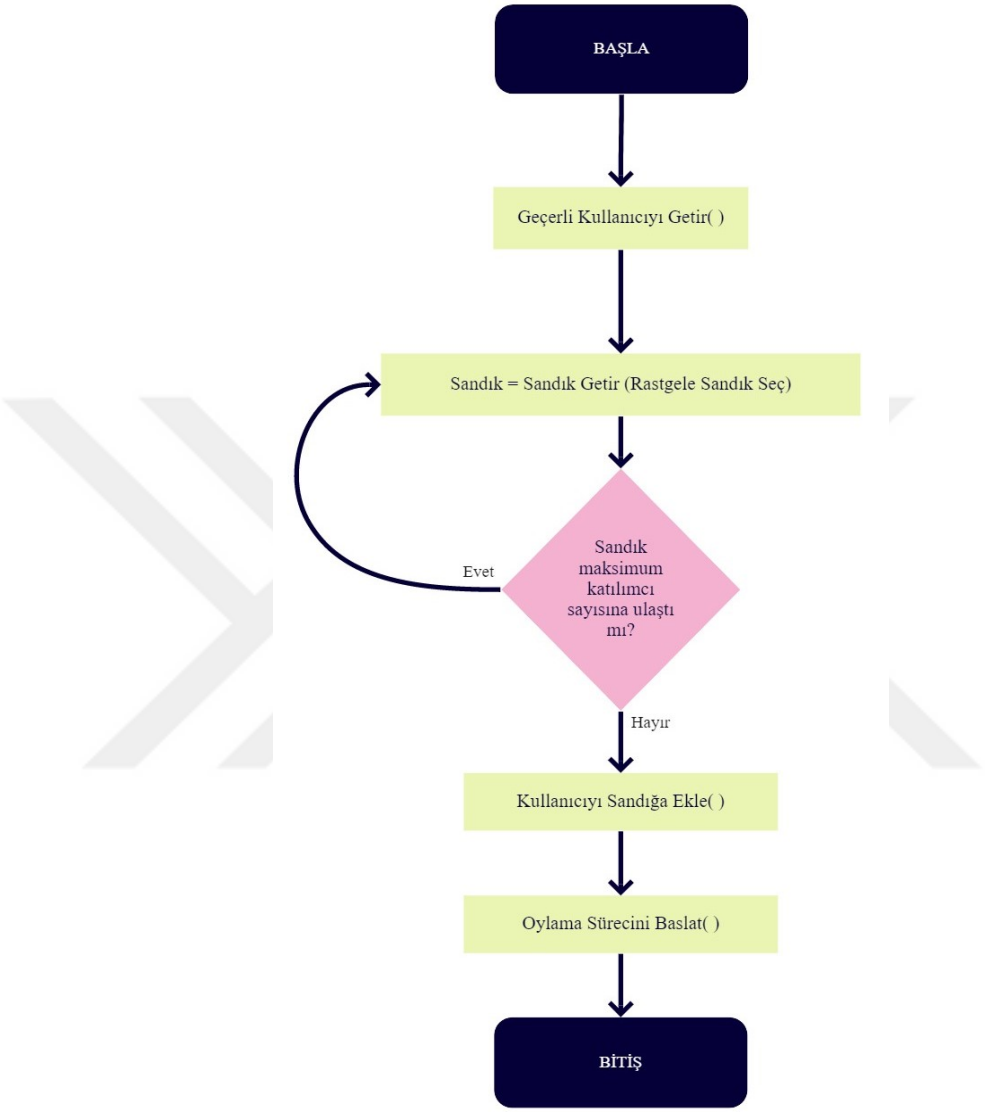
Sandık içerisinde yer alacak katılımcı sayısı açılacak olan maksimum sandık sayısına bölünerek ortalama katılımcı sayısı bulunur. Sandık sayınının belirlenmesinde olabileceği gibi katılımcı sayısının belirlenmesi de ondalık değere sahip olması ihtimaldir. Bu durumda katılımcı sayısı da yukarı yuvarlanmalıdır.

Sandık içerisinde atanacak olan katılımcıların yuvarlama işlemlerinden sonra kalan katılımcılar ile son sandık oluşturulur. Eğer son sandıktaki katılımcı sayısı 1 olması durumunda (on binlerce kişinin katılımı olacak oylama sistemi) ise WebRTC katılımcı sayısı 1 düşürülerek sandık sayısı artırılır, böylece son sandık içerisindeki katılımcı sayısının 10'dan büyük olması sağlanır.

Örnek olarak 2007 kişi ile yapılacak bir oylama sisteminde maksimum 256 katılımcı sayısı ile açılması gereken sandık sayısı 7.83 olarak çıkar. 0.83 sandık diye bir tanımlama yapılamayacağı için sandık değerlerinde yuvarlama işlemi yapılmalıdır. Aşağı yuvarlanma yapılırsa 7 sandık açılması yani (7 x 256 = 1792) katılımcı sayısına ulaşılır. Aşağı yuvarlama ile oylama sistemine giremeyecek 215 katılımcı ile adil ve demokratik bir seçim ortamı oluşturulamaz. Sandık ondalık değerleri yukarı yuvarlama yapılmalı çünkü WebRTC ile kullanıcı sayısı 256'nın altında olabilir, yukarı yuvarlanması ile 8 sandık açılması gerekir. Yuvarlama ile 7 sandık içinde 251,

son sandıkta 250 kullanıcı olarak oylama sistemi tamamlanabilir. Böylece her bir sandık içerisindeki katılımcı seviyesi azami değerde korunmuş olacaktır.

5.1.4 Oylama sürecine geçilmesi katılımcıların sandıklara atanması



Şekil 18: Yetkilendirme almış katılımcının rastgele sandık ataması

Sandıkların yetkilendirilmiş kullanıcılardan oluşturulmasından sonra oylama sürecine geçilir, Şekil 18'de gösterildiği üzere kullanıcının rastgele bir sandığa atanma süreci başlatılır.

Sistemden rastgele bir sandık isteği yapıldıktan sonra "Sandık maksimum katılımcı sayısına erişti mi?" sorusuna cevap hayır ise sistemden başka bir sandık istenir. Süreç maksimum katılımcı sayısına erişmemiş sandık bulunana kadar tekrarlanır. Uygun

sandık bulununca geçerli kullanıcının sandığa ataması yapılır ve kullanıcı için oylama süreci başlatılmış olur.

5.1.5 Sandık içinde oylama sürecinin başlaması

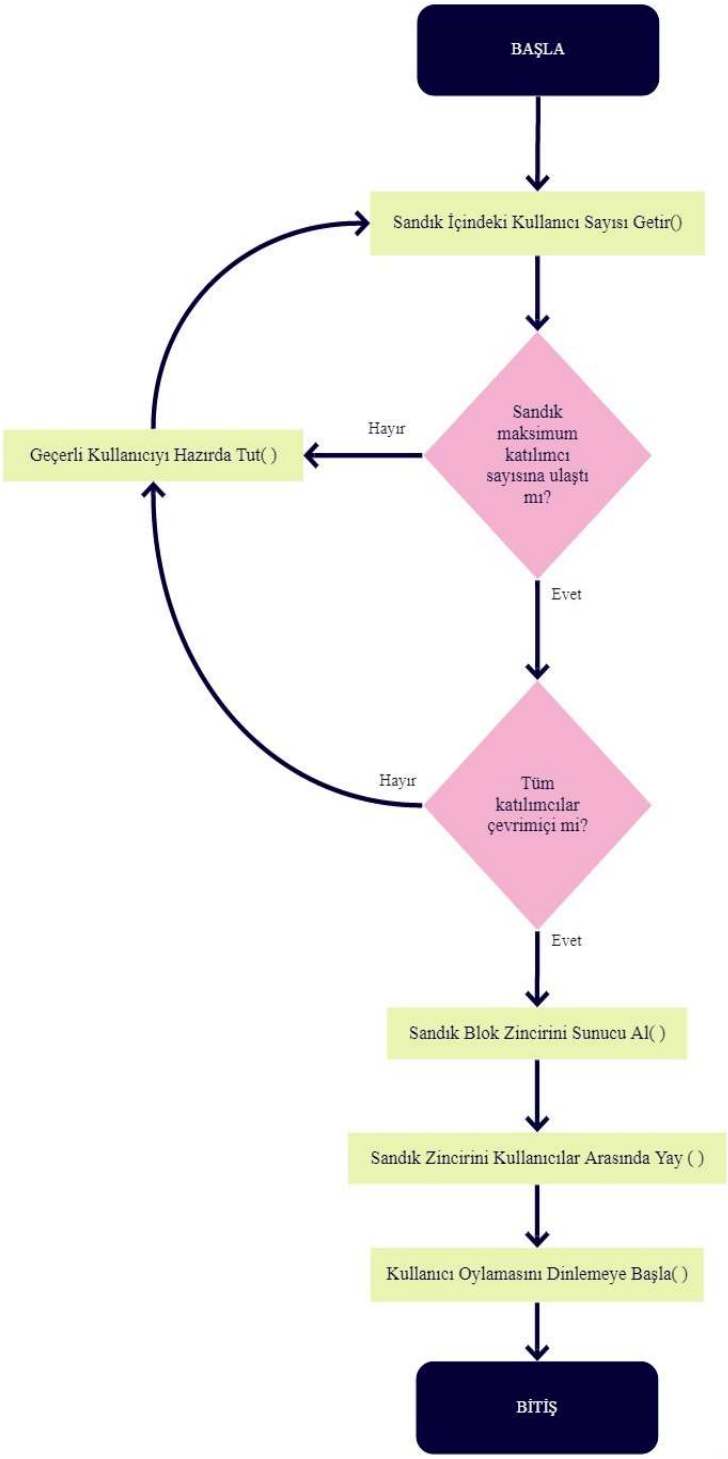
Şekil 19'da gösterilen akış şemasında sandık içerisindeki maksimum katılımcıya ulaşması ile oylama sürecinin başlatılması gösterilmiştir.

Mevcut sandık içerisinde katılımcı sayısı sistemden istenir. Bu sayı ile "Sandık maksimum katılımcı sayısına ulaştı mı?" sorusu yanıtlanır. Cevap "Hayır" ise geçerli kullanıcının durumu oylama için hazır konumda tutulmaya devam edilir. Cevap "Evet" ise ikinci koşula akış yönlendirilmesi sağlanır.

İkinci koşul içerisinde "Tüm katılımcılar çevrimiçi mi?" sorusu cevaplanır. Cevap "Hayır" ise ilk koşulun yönlendirildiği gibi akışta geçerli kullanıcının hazır konumda tutulma süreci devam ettirilir. Cevap "Evet" ise sandık içerisindeki katılımcılar maksimum seviyeye ulaşmış ve herkesin çevrimiçi olması sağlanmıştır.

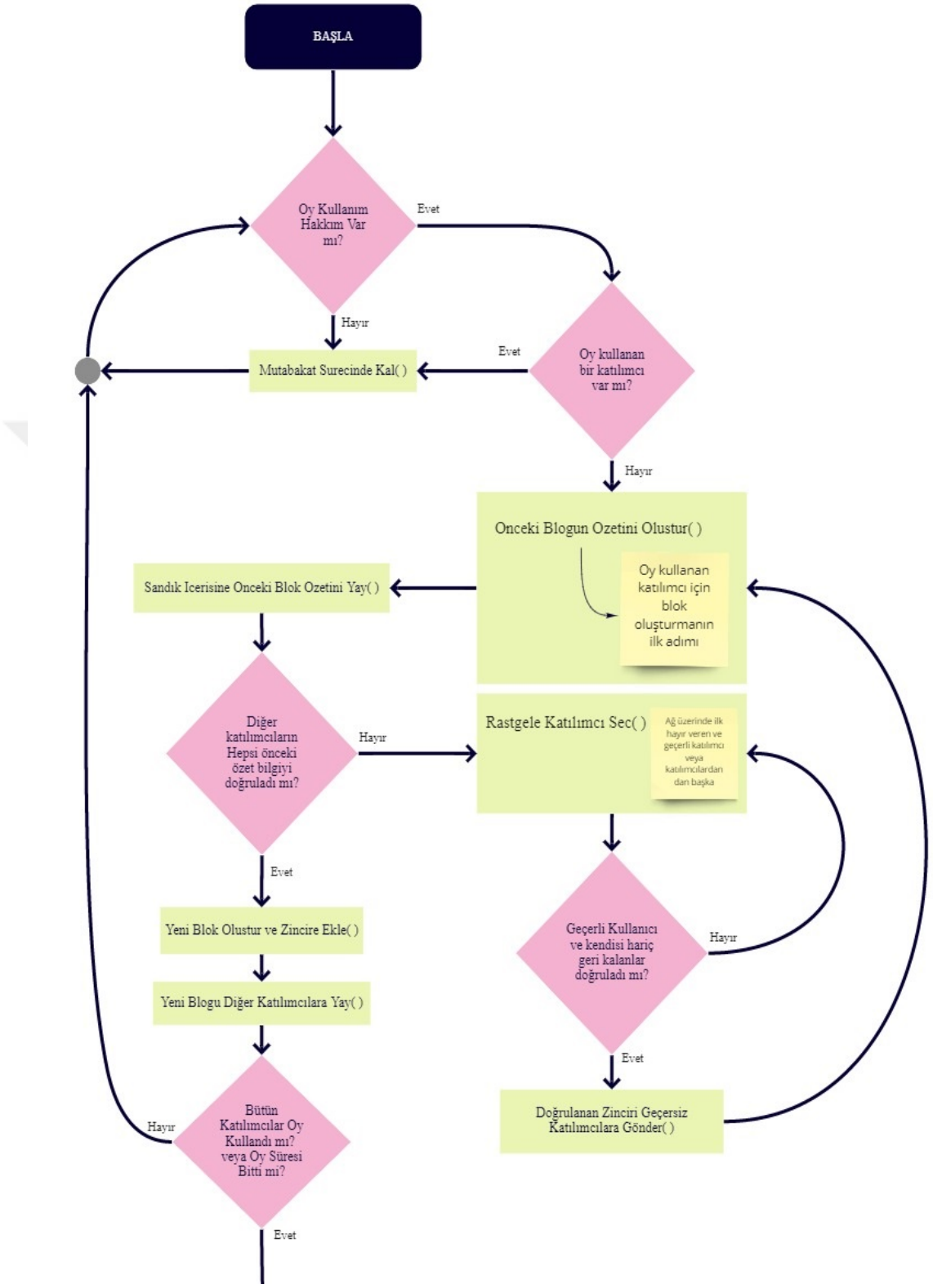
Sandık içinde oylama sürecinin başlaması için gerekli olan maksimum katılımcıya erişmiş olması ve bütün katılımcıların çevrimiçi olması ile sunucudan sandığa özel bir boş blok zinciri oluşturulması istenir. Bu istek sadece oylama sürecinin başlamasından önce gerçekleşir. Sunucudan alınan boş blok zincirine has olan genesis blok ile gelir. Genesis blok, kendisinden önceki bloğun özet (hash) bilgisini barındırmaz, blok zincirinin 0'ıncı elemanıdır. Kendisinden önce blok bulunmaz.

Sunucudan alınan genesis bloğa sahip blok zinciri katılımcının cihazına kaydedilir. WebRTC sayesinde alınan blok zinciri tüm katılımcılar arasında paylaşılır. Paylaşımdan sonra katılımcı oylama etkinliğine hazır konuma geçer ve ağı dinlemeye başlar. Blok zincirini alan katılımcı, zinciri kendi cihazına kaydeder ve diğer katılımcılar da oylama etkinliğine hazır konuma geçerler. Bu aşamada blok zinciri tabanlı WebRTC ile gerçek zamanlı çevrimiçi oylama sistemi altyapısal olarak tamamlanmış olmaktadır. Tüm katılımcılar sandık içerisinde eşten eşe bağlı durumda ağ üzerinde mutabakata hazır konumdadırlar.

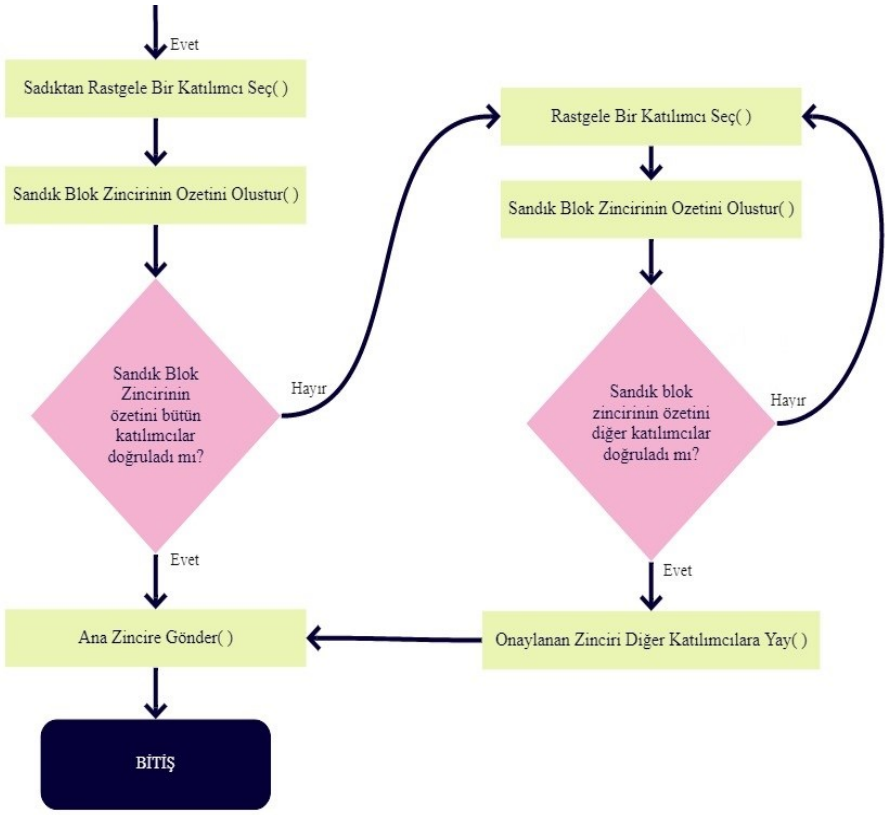


Şekil 19: Sandık maksimum katılımcı sayısına ulaşınca oylama sürecinin başlatılması

5.1.6 Sandık içinde oylama sürecinin tamamlanması



Şekil 20: Sandık içerisinde oylama etkinliğinin sürdürülmesi



Şekil 21: Şekil 20'in devamı olarak sandığın kapatılması ve ana zincire gönderilmesi

Şekil 20 ve devam görseli olan Şekil 21'de gösterilen akış şemasında sandık içerisinde yer alan katılımcıların oy verme ve diğer sandık içerisindeki katılımcıların etkinliklerini doğrulama süreçleri gösterilmiştir.

Gerçek zamanlı iletişime sahip sistemlerde bütün etkileşim, etkinliğin oluşturulduğu an gerçekleşir. Gerçek zamanlı iletişim sayesinde sandık içerisinde bulunan katılımcılar tüm etkinliklerden haberdar olabilmektedir. Oylama sürecinin başlaması ile birlikte katılımcının sistem üzerindeki etkin rolü başlamaktadır.

Akış içerisinde yer alan ilk koşulda katılımcının sandık içerisinde "Oy kullanım hakkım var mı?" sorusu ile katılımcının temel yönlendirilmesi yapılmaktadır. İlk koşulun cevabı "Hayır" ise katılımcı tercihini gerçekleştirmiş ve "Mutabakat

Sürecinde Kal( )" fonksiyonu ile doğrulama sürecinde kalması sağlanır. İlk koşulun çıktısı "Evet" ise akışta yer alan ikinci koşul kontrol edilir. İkinci koşul içerisinde yer alan "Oy kullanan bir kullanıcı var mı?" cevabı "Evet" ise ilk koşulun "Hayır" yönlendirilmesindeki aynı akışa yönlendirilerek katılımcının doğrulama sürecinde kalması sürdürülür. Katılımcının oy kullanım hakkı olduğu ve ağ üzerinde herhangi bir katılımcı etkinliğinin o anda bulunmadığı durumda ikinci koşulun "Hayır" akışı ile katılımcı oy verme sürecine geçişi "Önceki Bloğun Özetini Oluştur( )" fonksiyonu ile sağlanır.

"Önceki Bloğun Özetini Oluştur( )" fonksiyonu ile katılımcı sahip olduğu sandığa özel blok zincirinden son bloğu kullanarak SHA256 algoritması ile sabit uzunlukta özet (hash) bilgisi oluşturur. SHA256 algoritması herhangi bir uzunlukta veri olsa dahi on altılık sayı sisteminde her zaman 64 karakterlik çıktı üretmektedir. Veriler değişmediği sürece SHA256 algoritmanın çıktısı her zaman sabit olacaktır. Veri içerisinde en ufak bir değişiklik bile algoritmanın başka sonuç üretmesini sağlar. Böylece katılımcılar arasındaki farklılık tespit edilmiş olur. Özet üretildikten sonra akış "Sandık İçerisine Önceki Blok Özetini Yay( )" fonksiyonuna yönlendirilir.

"Sandık İçerisine Önceki Blok Özetini Yay( )" fonksiyonu ile WebRTC alt yapısı sayesinde katılımcılara üretilen 64 karakter uzunluğundaki özet bilgisi gönderilir. Fonksiyon sonucunda elde edilen bilgi "Diğer katılımcıların hepsi önceki özet bilgiyi doğruladı mı?" koşulu ile akış devam ettirilir.

"Diğer katılımcıların hepsi önceki özet bilgiyi doğruladı mı?" koşulun cevabı ağ üzerinde ilk "Hayır" cevabı veren ve geçerli katılımcıdan başka rastgele bir kullanıcı seçilerek önceki bloğun özet bilgisinin üretilmesi istenir. Rastgele kullanıcının ürettiği özet bilgisi geri kalan (mevcut katılımcı ve doğrulamaya hayır cevabı veren katılımcılar haricindeki) sandık katılımcılarına gönderilir. Bu süreç kalan katılımcıların onayladığı zincir tespit edilene kadar tekrarlanır. Böylece sandık içerisinde çoğunluk tarafından doğrulanmış manipüle edilmesi zorlaştırılmış güvenlik mekanizması sağlanmış olur. Çoğunluğun doğrulamış olduğu blok zinciri önceki

zincirleri doğrulanmayan katılımcılar mevcut katılımcı dâhil olarak aralarında paylaştırılır ve mevcut katılımcı “Önceki Bloğun Özetini Oluştur( )” akışına tekrar yönlendirilmesi yapılır.

Tekrarlanan bu mevcut kullanıcı tekrar sahip olduğu bloktan özet oluşturur ve ağda kontrol edilme süreci devam eder. Tüm katılımcılar bu doğrulamayı yaptığında ise mevcut katılımcı “Yeni Blok Oluştur ve Zincire Ekle( )” fonksiyonu ile yeni bir blok oluşturarak sahip olduğu zincire ekler. Zincire eklediği anda katılımcının oy kullanım hakkı sıfırlanır. Yeni oluşturduğu blok bilgisini ağ üzerindeki katılımcılara paylaşımını “Yeni Bloğu Diğer Katılımcılara Yay( )” fonksiyonu ile yapar. WebRTC ile gelen bu blok bilgisini katılımcılar kendi sahip oldukları zincire eklenmesini gerçekleştirirler ve katılımcı akışı “Bütün Katılımcılar Oy Kullandı mı veya Oy Süresi Bitti mi?” koşuluna yönlendirilir.

“Bütün Katılımcılar Oy Kullandı mı veya Oy Süresi Bitti mi?” koşunun cevabı “Hayır” ise katılımcı için süreç en baştaki “Oy Kullanım Hakkım Var mı?” koşuluna yönlendirilir. Zira bu aşamada katılımcı için oylama süreci sona ermiş sadece ağ üzerinde diğer katılımcı oylama süreçlerinde doğrulama yapmakla görevlidir. Cevap “Evet” ise Şekil 22’de gösterilen sandığın kapatılması ve ana zincire gönderilme süreci başlatılır.

Geçerli sandığın ana zincire gönderilme süreci “Sadıktan Rastgele Bir Katılımcı Seç( )” fonksiyonuna ile başlamaktadır. Ağ üzerinden rastgele bir katılımcı seçilir ve kullanma etkinliğinde olduğu gibi sahip olduğu blok zincirini kullanarak özet (hash) bilgi oluşturur. Bu özet bilgi ağdaki katılımcılara gönderilerek hepsinden doğrulama beklenilmektedir. Herhangi bir katılımcı doğrulamadığında bir önceki adımda seçilen rastgele katılımcı ve doğrulamayan katılımcıdan hariç olarak akış “Rastgele Bir Katılımcı Seç( )” fonksiyonuna yönlendirilir.

“Rastgele Bir Katılımcı Seç( )” ile katılımcı sırasıyla blok zinciri özeti oluşturur ve (rastgele katılımcı ve doğrulamaya hayır cevabı veren katılımcılar haricindeki) diğer sandık katılımcıları arasında doğrulanması gerçekleştirir. Bu süreç çoğunluk tarafından onaylanan blok zinciri tespit edilene kadar tekrarlanır.

Tespit edilen doğrulanmış blok zinciri ağ üzerindeki diğer doğrulamama yapamamış katılımcılar arasında "Onaylanan Zinciri Diğer Katılımcılara Yay( )" fonksiyonu ile yayılır. Katılımcılar arasında nihai olarak sonlandırılması yapılmış olan sandık blok zinciri "Ana Zincire Gönder" fonksiyonu ile katılımcıların arasından rastgele seçilmiş ana blok zinciri doğrulayıcılarına gönderilir.

Sandık içerisinde devam eden etkinlik süresince katılımcıların çevrimiçi kalması önem arz etmektedir. Bu önemli süreçte maksimum çevrimiçi katılımcı ile maksimum güvenli sistem oluşturulması sağlanır ve sistemin manipüle edilmesi zorlaştırılır.

5.1.7 Tamamlanan sandıkların ana blok zincirine dâhil edilmesi

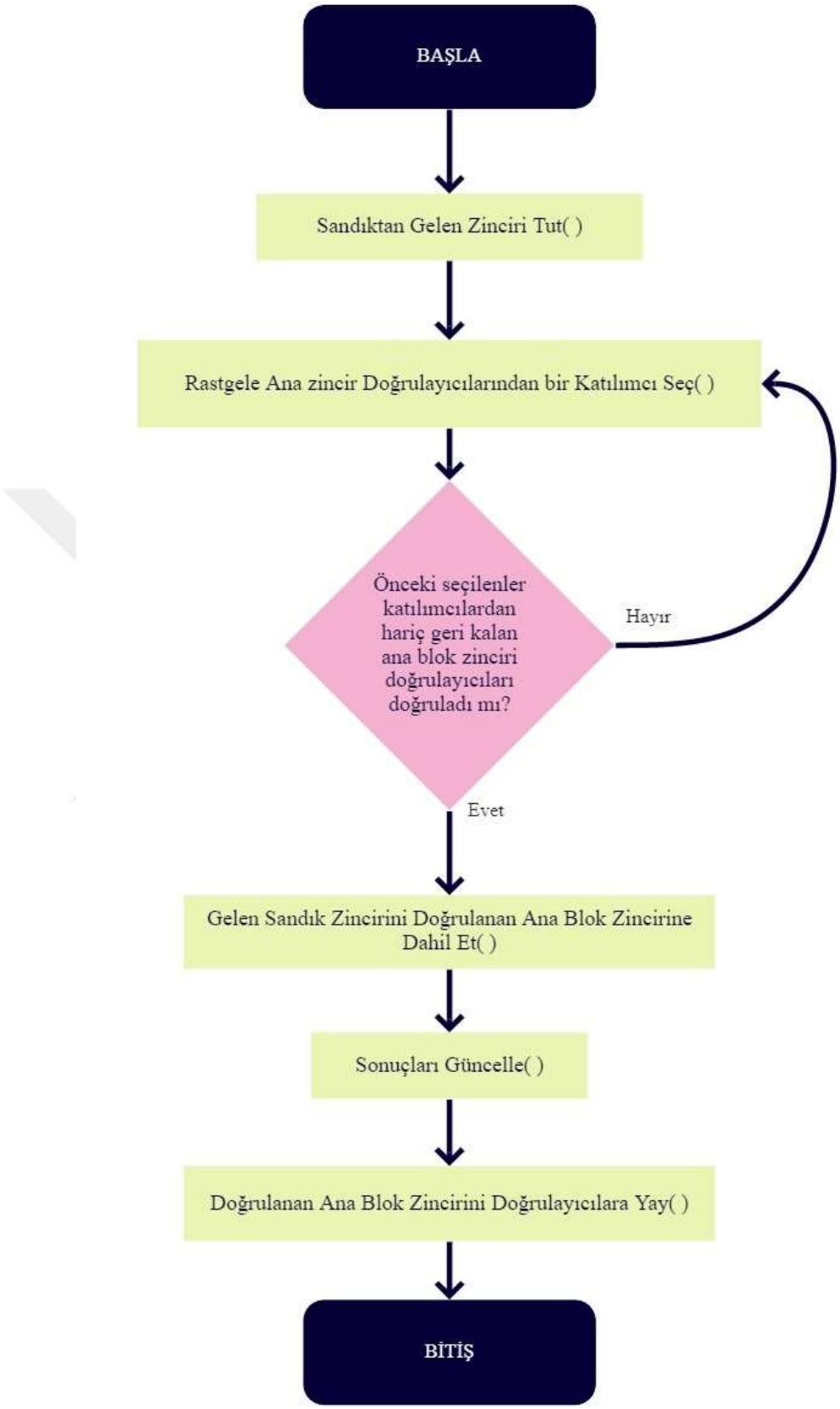
Şekil 22'de gösterilen akış şemasında sandık içerisinde oylamanın tamamlanması veya oylama süresinin bitmesinden sonraki sandık blok zincirinin oylama sistemin toplamının barındırıldığı ana blok zincirine eklenme süreci gösterilmiştir.

Sandık içerisindeki tüm katılımcıların onayladığı zincir oylama etkinliği oluşturulurken belirlenen ana zincir doğrulayıcılarının bulunduğu ağa yayılır. Ağ üzerinde ana zincir doğrulayıcılarının arasından rastgele bir katılımcı seçilir ve sahip olduğu blok zincirinden bir özet bilgi oluşturulması istenir.

Önceki akışlarda olduğu gibi katılımcıdan elde edilen ana blok zinciri özeti ağda bulunan diğer katılımcılar arasında yayılarak onaylanma sürecine gerçekleşir. Katılımcılar arasında fikir birliğine varılamaz ise onay vermeyen katılımcı ve ana blok zincirini üreten rastgele katılımcıdan hariç ağ üzerinden başka bir katılımcı seçilir. Onay süreci, yeni seçilen katılımcı ve önceki katılımcılar hariç tutularak devam eder. Geri kalan katılımcıların arasında doğrulanan zincir, önceki doğrulayamayan katılımcılar arasında yayılır.

Kapanan veya tamamlanan sandık verisi onaylanan ana blok zincirine eklenir. Gelen sandık zincirinin eklenmiş olan ana blok zincirinin bu süreçteki nihai hali ile güncel sonuçlar zincir üzerinde güncellenerek diğer katılımcılar arasında yayılır. Böylece kayıtların son hali ana zincir doğrulayıcıları arasında dağıtık olarak tutulması sağlanmış olur.

Oylama sisteminde açılmış olan bütün sandıklar tamamlandığında veya oylama süresi bittiğinde her bir sandık Şekil 22'de yer alan akış tekrarlanacaktır.



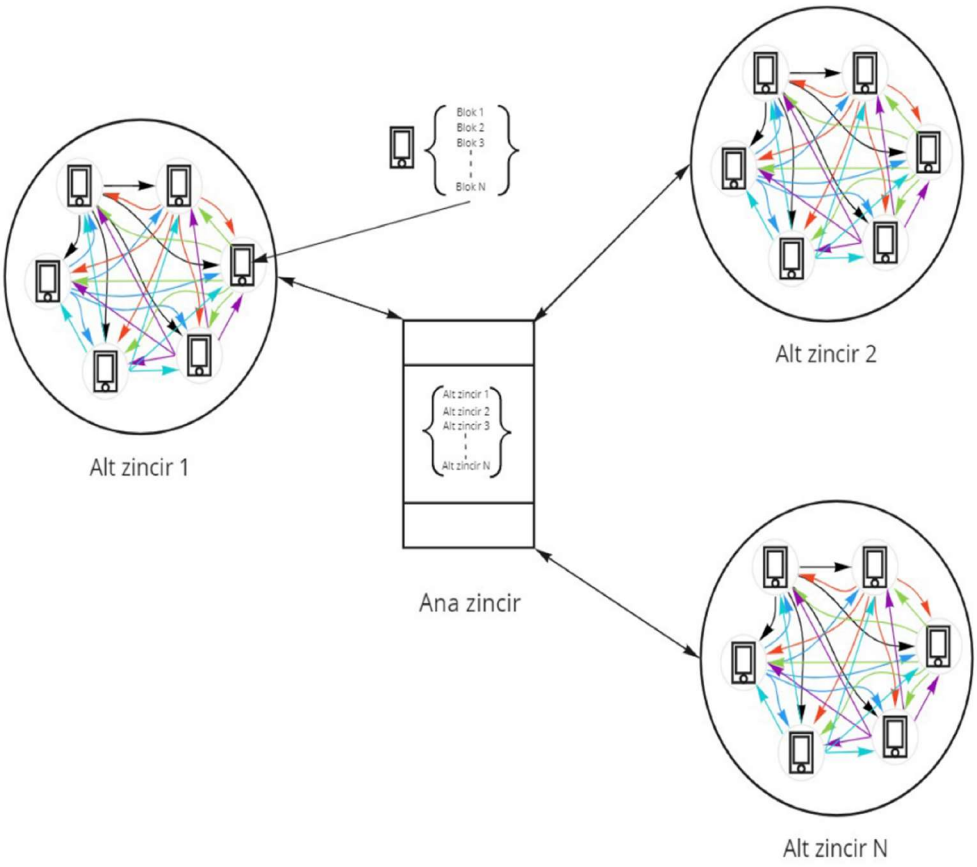
Şekil 22: Tamamlanan veya kapanan sandıkların ana blok zincirine eklenmesi

5.1.8 Oylama sürecinin sonlandırılması

Ağ üzerinde bulunan ana blok zinciri bütün sandıkların kapanması ile nihai haline ulaşır ve son sonuçların hesaplanması kısa sürede gerçekleşebilir. Elde edilen sonuçların doğruluğu ve güvenliği ağ katılımcıları arasında fikir birliğine varılması ile sağlanabilir. Ayrıca zincir üzerinde sonuçlar hakkında; toplam kaç oy kullanıldığı, oylamanın sonuçları, oylama süresi gibi çeşitli istatiksel veriler üretilebilir.

5.1.9 Çevrimiçi oylama sistemi topolojisi

Sistem aşamalara uygun olarak tamamladığında Şekil 23'te gösterildiği gibi bir altyapı oluşacaktır. Alt zincirler oylama etkinliği oluşturulduktan sonra çevrimiçi olan katılımcı sayısına göre açılacak olan sandıklardır. Katılımcılar arasında dağıtık olan yapı görünmekte, sandık kapandığında ise ağ üzerinde bulunan herhangi bir ana zincire dâhil olma gösterilmiştir.



Şekil 23: Altyapı temsili gösterimi

6. BULGULAR VE YORUMLAR

Bu bölümde araştırma kapsamında elde edilen bulgulara ve yorumlar yer almaktadır.

6.1 Arkaplan

6.1.1 Akıllı telefonların evrimi

Teknolojinin hızla ilerlemesi ve maliyetlerin azalmasıyla birlikte akıllı telefonların kullanım alanları da hızlıca artmıştır. Bu durum akıllı telefonların gündelik hayatın içerisinde fazla yer edinmesini sağlamıştır.

Günümüzdeki akıllı telefonları başlangıcı ilk nesil olan cep telefonlarıdır. 1G, 2G, 3G, 4G ve 5G olarak isimlendirilen GSM teknolojilerinde G (nesil) olarak ifade edilmektedir. Her bir nesil kendisinden önceki nesilden oldukça hızlı olup yeni uygulamaların geliştirilmesine zemin sağlamıştır.

1G birinci nesil sistemler sadece analog sistemle çalışmakta olup sadece ses taşıması için tasarlanmış olup 1980 yılından 1990 yılının başlarına kadar kullanılmıştır.

2G ile GSM teknolojisi dünya genelinde yaygınlaşmasını sağlayan sayısal haberleşme ile GSM teknolojilerinin temel yapısını oluşturmuştur. 64- 384 Kbps aralığına veri hızına sahiptir. SMS gönderip alma özelliği 2G ile gelen yeniliktir. 1990 yılından 2000 yılının başlarına kadar kullanılmıştır.

3G ile cep telefonları akıllı hale gelmişlerdir. Ses ve görüntü gönderimleri sağlanırken telefonlar üzerinde internet tarayıcıları, web tabanlı oyunlar ve VoIP uygulamaları kullanılmaya başlamıştır. HSPA 3.5G ismi ile 14 Mbps, HSPA+ 3,75 G isimlendirilmesiyle de 168 Mbps hızlarına kadar ulaşmıştır.

4G altyapısı ile akıllı telefonlar 3G'ye göre daha yüksek hızda veri gönderimi yapabilir hale gelmiştir. IP tabanlı olarak çalışmaktadır. LTE+ teknolojisi ile adı 4.5G olarak anılmaya başlamış 1Gbps hızlarına kadar çıkabilmektedir.

Günümüzde 5G ile 20 Gbps'e kadar veri gönderimi yapabilmektedir. Bu nesilde düşük enerji tüketimi ve düşük gecikmeli iletim sayesinde nesnelerin interneti (IoT) teknolojilerinin hızla gelişmesine yardımcı olmaktadır.

Akıllı telefonların günümüzde geldiği noktada uygulama marketleri oyunlara ve uygulamalara, tarayıcılar sayesinde ise internete açılan kapılardır.

6.1.2 Dünyada akıllı telefon kullanımı

Tablo 2'de Newzoo'nun yayınlamış olduğu "2019 Free Global Mobile Market Report" raporunda dünya çapında en çok aktif kullanıcıya sahip olan 20 ülke yer almaktadır. Çin, 2019'un sonunda 851 milyondan fazla akıllık telefon kullanıcısı ile dünya sıralamasında birinci ülke olmuştur İkinciliği 345 milyondan fazla kullanıcısı ile Hindistan, üçüncülüğü de 260 milyondan fazla kullanıcısı ile Amerika Birleşik Devletleri olmuştur [34].

Ülke	**Sıralama**	**Nüfus**	**Akıllı Telefon Kullanıcısı**	**Nüfusun Oranı**
Çin	1	1420 milyar	851,2 milyon	%59,9
Hindistan	2	1368 milyar	345,9 milyon	%25,3
ABD	3	329,1 milyon	260,2 milyon	%79,1
Brezilya	4	212,4 milyon	96,9 milyon	%45,6
Rusya	5	143,9 milyon	95,4 milyon	%66,3
Endonezya	6	269,5 milyon	83,9 milyon	%31,1
Japonya	7	126,9 milyon	72,6 milyon	%57,2
Meksika	8	132,3 milyon	65,6 milyon	%49,5
Almanya	9	82,4 milyon	65,9 milyon	%79,9
Birleşik Krallık	10	67 milyon	55,5 milyon	%82,9
Fransa	11	65,5 milyon	50,7 milyon	%77,5

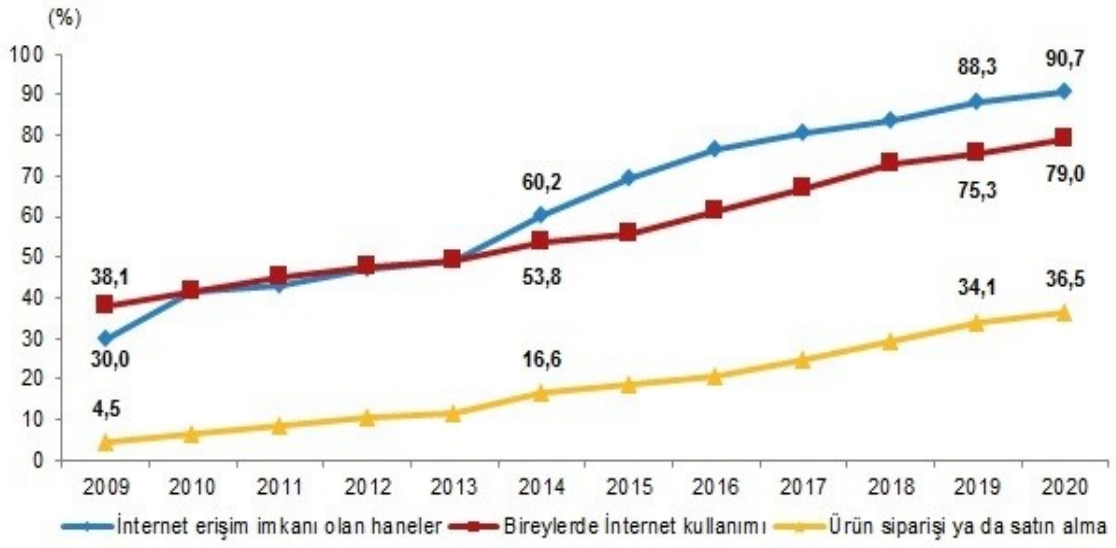
İran	12	82,8 milyon	45,4 milyon	%54,8
Türkiye	13	83 milyon	44,8 milyon	%54
Vietnam	14	97,4 milyon	43,7 milyon	%44,9
Filipinler	15	108,1 milyon	36,3 milyon	%33,6
Güney Kore	16	51,3 milyon	36,1 milyon	%70,4
İtalya	17	59,2 milyon	36 milyon	%60,8
Pakistan	18	204,6 milyon	32,5 milyon	%15,9
İspanya	19	46,4 milyon	34,5 milyon	%74,3
Bangladeş	20	168,1 milyon	31 milyon	%18,5

Tablo 2: Newzoo 2019 raporunda en çok akıllı telefon kullanan dünyada ilk 20 ülke

6.1.3 Türkiye'de akıllı telefon kullanımı ve internete erişim

"We are social 2020" raporuna göre 2020'de Türkiye'de mobil kullanıcı sayısı artarak 58.23 milyona ulaşmış durumdadır. Aynı raporda yer alan başka bir sonuca göre Türkiye'de mobil internet kullanan kullanıcıların sayısı toplam internet kullanan kullanıcı sayısına oranı ise %94 olmuştur [35].

Ağustos 2020 itibariyle Şekil 24'te gösteriliği gibi Türkiye'de özellikle hanelerin %90,7'sinde evden internete erişim olduğu TÜİK raporunda yer almıştır. İlgili raporda internet kullanan bireylerin 16-74 yaş aralığındaki oranının ise %79 olduğu belirtilmiştir [36].



Şekil 24: TÜİK Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması [36], 2020

6.1.4 Oy kullanım ölçütlerinin sağlanması

Tablo 3'te belirtildiği üzere adil olarak demokratik bir seçim yapılabilmesi için oy verme sistemlerinin bazı ölçütlerin sağlamış olması gerekmektedir [5].

Oy kullanım ölçütleri	**Blok zinciri**	**WebRTC**	**Kimlik Doğrulama**
Yeterlilik ve doğrulama			X
Güvenilirlik	X	X	X
Bütünlük	X	X	
Şeffaflık	X	X	
Denetime Açık	X		X
Gizliliğin Sağlanması	X	X	X
Baskı Altına Alınmaması		X	X
Esneklik		X	
Kolaylık	X	X	X

Onaylanabilme	X	X	X
Maliyet	X	X	X

Tablo 3: Oy kullanım ölçütleri [5]

Yeterlilik ve doğrulama süreci, kişinin oy kullanabilmesi için gerekli vasıflara sahip olup olmaması, sistem üzerinde kimlik doğrulama ile çözümlenmiştir.

Güvenilirlik, katılımcının doğrulanmış olması, blok zincirinin değiştirilemez kronolojik yapısı ve WebRTC ile eşler arasında dağıtık fikir birliği dâhilinde verinin gizli tutulması ile çözümlenmiştir.

Bütünlük, blok zinciri teknolojisinin blokların bir önceki verinin özet bilgisi (hash) ile oluşturulması ardı ardına eklenmesi ve bu blokların WebRTC ile eşler arasında fikir birliği ile sağlanması ile çözümlenmiştir.

Şeffaflık, uygulama süresince bütünlük ve güvenilirlik maddeleriyle manipülasyon maliyetinin çok fazla olması sonuçların anlık olarak hesaplanması ile çözümlenmiştir.

Denetime açıklık, blok zinciri ve kimlik doğrulanması olan katılımcıların anlık geriye dönük verileri tekrar gözden geçirilebiliyor olması ile çözümlenmiştir.

Gizliliğin sağlanması, çevrimiçi oylama sisteminde kimlik doğrulamadan sonra birbirinden uzakta olabilen rastgele katılımcıların tek bir kümede toplanarak birbirleri arasında fikir birliği yapması ve katılımcı seçiminin blok zinciri üzerinde şifrelenerek tutulması sayesinde çözümlenmiştir.

Baskı altına alınamaması, kimlik doğrulama sonrası, çevrimiçi oylama süresince katılımcının konum bağımsızlığı, internete bağlı olabileceği herhangi bir yerde olması ile rastgele kullanıcılardan oluşturulmuş kümedeki katılımcıların birbirini bilemiyor olması, özgür bir seçim ortamı ile çözümlenmiştir.

Esneklik, katılımcı üst sınırı olmadan, WebRTC ile sandık sayıları artırılarak binlerce kullanıcının olduğu sandıklar dinamik olarak oluşturularak çözümlenmiştir.

Kolaylık, kapsamda artık ihtiyaç duyulmayacak olan oy pusulaları, birçok değişik yerlerde açılan sandıklar, gözetimcilerin fiziki olarak bulunmaması, blok zinciri üzerinde verilerin bütünlüğünün korunması, WebRTC ile verilerin eş zamanlı dağıtık tutuluyor olması, sayım yükünün otomatik olarak katılımcılar arasında paylaşılıyor olması ile çözümlenmiştir.

Onaylanabilme, kimlik doğrulama sonrası blok zincirine uygun yeni bir bloğun oluşturulması ve diğer katılımcıların bunu onaylaması ile çözümlenmiştir.

Maliyet, birçok yerde açılan sandıklar, gözetmen, sayım memurları, salon kiralama, matbaa, lojistik hizmet giderleri, temizlik, katılımcı bilgilendirme gibi büyük maliyetlerin artık olmaması ile çözümlenmiştir.

7. SONUÇ

Gelişen mobil iletişim teknolojileri ile yüksek hızda veri iletimleri ile ortaya çıkmasını sağladığı mobil aplikasyonlar sayesinde günlük hayattaki akıllı telefonların kullanımını artırmıştır. Bu kullanımlara örnek olarak e-devlet uygulamaları, sosyal medya platformları, mesajlaşma, oyunlar, şirketlerin personel ihtiyaçları veya müşteri gereksinimleri için geliştirmiş olduğu özel uygulamalar ile ortalama Türkiye'de akıllı telefon kullanım süresi 4 saatten fazla olmuştur [35].

Literatür araştırmaları sonucunda daha önce yapılmış olan öneriler ve çalışmalar blok zinciri tabanlı oy sistemlerinin güvenlik, şeffaflık, doğruluk, merkezi olmayan dağıtık yapıları kripto para teknolojileri üzerinde oluşturmuşlardır.

Oy kullanım ölçütlerine uygun olan blok zinciri ile veri güvenliğini sağlayan, WebRTC gerçek zamanlı iletişim teknolojisi ile katılımcılar arasında eşten eşe bağlı ve dağıtık mimari seçim oylama sistemi önerilmiştir. Eksik olan bu alandaki çalışmaların blok zinciri ve RTC teknolojileri birlikte kullanılarak kuramsal ve uygulamalı yeni çalışmaların yapılması önerilmektedir.

KAYNAKÇA

[1] **Zetter, K.,** (2012). "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners" Wired Magazine
https://www.wired.com/2012/07/reverse-engineering-iris-scans, 02.12.2020.

[2] **Tikveşli, O.A.,** (2019). Blok Zincir Teknolojisi ve %51 Sorunsalı.

[3] Blokzincir Teknolojileri, Bilgem, Tubitak
https://blokzincir.bilgem.tubitak.gov.tr/bz-calistay/blok-zincir.html, 02.12.2020.

[4] **Nakamoto, S.,** (2008) Bitcoin: A peer-to-peer electronic cash system.
https://bitcoin.org/bitcoin.pdf, 02.12.2020.

[5] **Akın, M.,** (2006), Elektronik Oy Verme Sistemlerinde Güvenlik: Deneyimler ve Türkiye İçin Öneriler.

[6] Enterprise-grade Hybrid Blockchain Platform (2020)
https://wavesenterprise.com/we-whitepaper-en.pdf, 02.12.2020.

[7] **Yanovich, Y., Ivashchenko, I., Ostrovsky, A., Shevchenko, A., Sidorov, A.,** (2018), Exonum: Byzantine fault tolerant protocol for blockchains
https://exonum.com/theme/public/img/downloads/wp_consensus_181227.pdf, 02.12.2020.

[8] "Volgograd bölgesinde katılımcı bütçeleme oylama"
https://polys.me/success-stories/volgograd, 02.12.2020.

[9] **Nagey, S.,** Version 1.1 (2016), Software That Powers Democracy Should Be Free
http://inno.vote/whitepaper/Inno.vote%20%E2%80%94%20Bringing%20Democracy%20to%20Elections.pdf, 02.12.2020.

[10] Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability (2020)
https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf, 02.12.2020.

[11] **Specter, A. M., Koppel, J., Weitzner, D.** The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf, 02.12.2020.

[12] **AKI, J.** (2018) Switzerland's "Crypto Valley" Successfully Completes Blockchain Voting Trial

https://bitcoinmagazine.com/articles/switzerlands-crypto-valley-successfully-completes-blockchain-voting-trial, 02.12.2020.

[13] **AKI, J.** (2018) Thailand Uses Blockchain-Supported Electronic Voting System In Primaries

https://bitcoinmagazine.com/articles/thailand-uses-blockchain-supported-electronic-voting-system-primaries, 02.12.2020.

[14] **Rosic, A.** What is Blockchain Technology? A Step-by-Step Guide For Beginners https://blockgeeks.com/guides/what-is-blockchain-technology, 02.12.2020.

[15] **Tanrıverdi, M., Uysal, M., Üstündağ, T. A.,** (2019) Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi, Bilişim Teknolojileri Dergisi Cilt:12, Sayı:3, Sayfa:203.

[16] **Ray, S.,** (2017) Blockchains versus Traditional Databases https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79, 02.12.2020.

[17] **Ünal, G., Uluyol, Ç.,** (2020) Blok Zinciri Teknolojisi, Bilişim Teknolojileri Dergisi Cilt:13, Sayı:2, Sayfa:167.

[18] **Shihab, S. H., Qusay, H. M.** (2019) Comparative evaluation of consensus mechanismsin cryptocurrencies

https://onlinelibrary.wiley.com/doi/epdf/10.1002/itl2.100, 02.12.2020.

[19] **Cook, D. J.** (2018) What is proof-of-work?

https://www.johndcook.com/blog/2018/11/11/proof-of-work, 02.12.2020.

[19] **King, S., Nadal, S.** (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake

https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf, 02.12.2020.

[21] Proof of Stake (PoS)

https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake, 02.12.2020.

[22] **Yi, S., Lingjun, F., Hong, X.** (2018) Technology Development and Application of Blockchain: Current Status and Challenges.

[23] **Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.** (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data.

[24] Technology – Delegated Proof-of-Stake Consensus

https://how.bitshares.works/en/master/technology/bitshares_features.html, 02.12.2020.

[25] Bitcoin Blockchain Size

https://ycharts.com/indicators/bitcoin_blockchain_size, 02.01.2020.

[26] Ethereum Full Node Sync (Default) Chart

https://etherscan.io/chartsync/chaindefault, 02.01.2020

[27] Web için gerçek zamanlı iletişim, https://webrtc.org, 02.01.2020

[28] WebRTC Peer-to-peer connections, https://caniuse.com/?search=webrtc, 02.01.2020

[29] WebRTC Basic Concept , https://bloggeek.me/how-webrtc-works, 02.01.2020

[30] **Grigorik, I.** WebRTC https://hpbn.co/webrtc, 02.12.2020.

[31] Medya yakalama ve kısıtlamalar

https://webrtc.org/getting-started/media-capture-and-constraints, 02.12.2020.

[32] **Aydın, A.,** (2008), 1982 Anayasası Sonrası Siyasi Partiler ve Seçim Sistemi

[33] WebRTC 1.0: Real-Time Communication Between Browsers

https://www.w3.org/TR/2020/CRD-webrtc-20201203, 25.12.2020

[34] Newzoo Global Mobile Market Report 2019 | Light Version,

https://newzoo.com/insights/trend-reports/newzoo-global-mobile-market-report-2019-light-version, 02.12.2020

[35] We Are Social 2020 Turkey, https://www.slideshare.net/DataReportal/digital-2020-global-digital-overview-january-2020-v01-226017535, 02.12.2020

[36] TÜİK Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması (2020) https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679, 02.12.2020

ÖZGEÇMİŞ