

Raft Tabanlı Alternatif Konsensüs Algoritmalarının Performans Analizi

Halil İbrahim Yılmaz^{1*}, Ahmet Coşkunçay²

¹Yazılım Mühendisliği/Mühendislik Fakültesi, Atatürk Üniversitesi, Erzurum, Türkiye(yilmaz.halil@atauni.edu.tr)

²Bilgisayar Mühendisliği/ Mühendislik Fakültesi, Atatürk Üniversitesi, Erzurum, Türkiye (ahmet.coskuncay@atauni.edu.tr)

Özet – Blokzincir teknolojileri, asimetrik şifreleme, hash algoritmaları, dağıtık yapı, akıllı sözleşmeler ve konsensüs mekanizmaları gibi kavramlara dayanır. Konsensüs mekanizmaları, blokzincir teknolojisi de dahil olmak üzere dağıtık sistemlerde, tüm düğümlerdeki verilerin aynı, doğrulanabilir, tutarlı ve geçerli sonuçlar üretmesini sağlayan yöntemlerdir. Bir blokzincir ağında, bilgilerin tüm düğümlerde tutarlı kalmasını garanti ederler. Raft gibi önde gelen oy tabanlı konsensüs protokolleri ise yaygın kullanılsalar da çeşitli dezavantajlar barındırmakta ve bazı yönlerden iyileştirmeye ihtiyaç duymaktadır. Özellikle tüm sorumluluğun lider düğüm üzerinde olması, düğümlerdeki itibar sorunları ve Bizans hata olasılığının varlığı gibi sorunlar, Raft konsensüs algoritması üzerinde iyileştirme çalışmalarına sebep olmuştur. Bu nedenle alternatif konsensüs protokollerinin ele alınması, sahip oldukları özgün tasarım nitelikleriyle, akademik çevreler, blokzincir alanındaki uygulayıcılar ve araştırmacılar için güncel gelişmelere katkı sağlamak ve alanın ilerlemesine olanak tanımaktadır. Bu çalışmada, oluşturulacak bir simülasyon içerisinde, Raft konsensüs algoritması temelli X-RAFT, RE-RAFT, RR-RAFT ve LRD-RAFT konsensüs algoritmalarının verim, gecikme metrikleri üzerinde performans analizi yapılarak, Raft algoritması üzerindeki iyileştirme girişimlerinin karşılaştırılması amaçlanmaktadır. Geliştirilen yeni konsensüs algoritmalarının performans ölçümüyle elde edilecek sonuçlar, oy tabanlı konsensüs algoritmalarının blokzincir ağları üzerinde performans anlamında fikir vermesi amaçlanmaktadır.

Keywords – blokzincir, konsensüs protokolü, raft, verim, gecikme

Performance Analysis of Raft-Based Alternative Consensus Algorithms

Abstract – Blockchain technologies are based on concepts such as asymmetric encryption, hash algorithms, distributed structure, smart contracts, and consensus mechanisms. Consensus mechanisms are methods that ensure that data in all nodes produce the same, verifiable, consistent, and valid results in distributed systems, including blockchain technology. In a blockchain network, they guarantee that information remains consistent across all nodes. Leading vote-based consensus protocols such as Raft, although widely used, have various disadvantages and need improvement in some aspects. In particular, problems such as the fact that all responsibility lies with the leader node, reputation problems in nodes, and the existence of the possibility of Byzantine errors have led to improvement studies on the Raft consensus algorithm. Therefore, considering alternative consensus protocols, with their unique design features, contributes to current developments for academic circles, blockchain practitioners, and researchers and allows the field to advance. In this study, it is aimed to compare the improvement attempts on the Raft algorithm by performing performance analysis on the throughput and delay metrics of the X-RAFT, RE-RAFT, RR-RAFT and LRD-RAFT consensus algorithms based on the Raft consensus algorithm in a simulation to be created. The results to be obtained by measuring the performance of the newly developed consensus algorithms are intended to give an idea about the performance of vote-based consensus algorithms on blockchain networks.

Keywords – blockchain, consensus protocol, raft, throughput, latency

I. GİRİŞ

Satoshi Nakamoto [1], 2008 yılında yayınladığı “Bitcoin: A Peer-to-Peer Electronic Cash System” başlıklı kitabında blokzincir teknolojisini ortaya koymuş, tanım olarak dağıtık defter teknolojisi üzerinde geliştirilen bir teknoloji olduğunu belirtmiştir. Beck ve arkadaşları [2], bu teknolojinin, merkezi otoritelere ihtiyaç duymadan güvenli ve şeffaf işlemler yapılmasını sağlayarak, süregelen finans sistemlerinde köklü bir dönüşümün temelini attığını ifade ettiler. Abeyratne ve arkadaşları [3], blokzincir teknolojisinin uygulama alanlarının geniş olduğunu ve sadece finans sektörüyle sınırlı olmadığını; tedarik zinciri analizi, akıllı sözleşmeler ve kimlik yönetimi gibi pek çok alanda dönüşüm potansiyeline sahip olduğunu ifade ettiler. FG DLT’de [4], dağıtık defterlerin, kamuya açık (public) ya da özel (private) olabileceği, kamuya açık

blokzincirlerin tüm kullanıcılara açık olduğu, özel blokzincirlerde ise yalnızca belirli kullanıcıların ağa dahil olabileceği belirtildi. Tschorsch ve arkadaşları [5], blokzincirin temel özellikleri arasında değişmezlik, kriptografik güvenlik ve dağıtık konsensüs mekanizmaları olduğunu belirtmişlerdir. Alzahrani ve arkadaşları [6], mutabakat protokollerinin, bir ağdaki katılımcı düğümlerin bir işlemin geçerli olup olmadığına karar vermek için kullandıkları bir dizi kural olduğunu belirterek, konsensüs protokollerinin tüm katılımcıların toplu olarak ortak bir dağıtık defteri tutmasını sağladığını ifade etmişlerdir. Hattab [7], mutabakat protokol mekanizmalarını donanımaya dayalı, oya dayalı ve hisseye dayalı olmak üzere 3’e ayırır. Başka bir çalışmada Nguyen ve arkadaşları [8], mutabakat protokol mekanizmalarını kanıt dayalı ve oya dayalı olmak üzere ikiye

ayırıştır. Bununla birlikte Wang ve arkadaşları [9], ölçeklenebilirlik (scalability), işlem hızı (throughput) ve enerji verimliliği (energy efficiency) gibi sorunlar, yeni konsensüs mekanizmalarının geliştirilmesini zorunlu kıldığını vurgulamışlardır. Raft algoritması, sadeliği ve uygulanabilirliği ile öne çıkmasına rağmen, Bizans hata toleransı eksikliği, sınırlı ölçeklenebilirlik ve lider düğüm üzerindeki yoğun işlem yükü gibi temel sınırlamalara sahiptir. Bu eksiklikler, ağ büyüklüğü arttıkça performans kaybına ve lider düğüm üzerindeki problemler, konsensüs gecikmelerine yol açmakta; dolayısıyla, yeni nesil konsensüs mekanizmalarının geliştirilmesini zorunlu kılmaktadır.

Konsensüs algoritmalarındaki bu tür sorunların giderilmesi, dağıtık sistemlerin genel güvenilirliğini ve dayanıklılığını güçlendirmek açısından kritik bir önem taşımaktadır. Zheng ve arkadaşlarına göre [10], literatürde, ölçeklenebilirlik, enerji verimliliği ve hata toleransı gibi temel gereksinimlerin karşılanması, konsensüs protokollerinin uzun vadeli etkinliği ve başarısı açısından kritik rol oynadığı vurgulanmaktadır.

Yeni geliştirilen alternatif konsensüs algoritmaları, Raft algoritmasının sınırlamalarını aşmayı ve özellikle ölçeklenebilirlik, işlem hızı ve hata toleransı gibi kritik alanlarda iyileştirmeler sağlamayı hedeflemektedir. Bu algoritmaların uygulanabilirliğini ve etkinliğini değerlendirmek amacıyla, Raft tabanlı ağlar üzerinde çeşitli performans testleri ve karşılaştırmalı analizler gerçekleştirilmesi planlanmaktadır. Yapılacak bu testler, ağ performansında gözlemlenen iyileşmeleri nicel verilerle ortaya koymayı amaçlamakta ve önerilen yaklaşımların teknik geçerliliğini desteklemektedir. Ayrıca, test sonuçları sistem güvenliği ve işlem sürekliliği açısından iyileştirmeler sağlayarak, konsensüs protokollerinin uzun vadeli başarısına katkı sunacaktır. Bu kapsamda önerilen yaklaşım hem teorik hem de pratik düzeyde ağ optimizasyonuna olanak tanımaktadır.

Lamport ve arkadaşları [11], Raft, Paxos kadar etkili olduğunu, Raft'ın Paxos'tan daha kolay anlaşılabilirliğini çünkü Raft'ın yapısının Paxos'tan farklı olduğu üzerinde durmuşlardır. Ni ve arkadaşları [12], Raft algoritmasının, replikasyon kayıtlarını yönetmek için kullanılan bir tutarlılık algoritması olduğunu ve algoritmaların seçim sınıfına ait olduğunu ileri sürmüşlerdir. Ongaro ve arkadaşları [13], Raft konsensüs algoritmasını, basitlik ve belirlenebilirliği ön plana çıkararak, fikir birliğine lider tabanlı bir yaklaşım olarak tanımlamışlardır. Düğümlerin, blok zinciri işlemlerini yönetecek bir lideri seçmek için oy kullandığı seçim temelli bir modelle çalıştığını söylediler. Bu tasarımın, izinli blok zinciri ortamlarında verimli karar almayı mümkün kıldığını; ancak, lider seçiminin belirleyici (deterministik) doğası bazı güvenlik açıklarına yol açabileceğini belirttiler. Liderin sık sık başarısız olması, tekrar eden seçim süreçlerine neden olabileceğini ve bu durumun gecikmelere, sistemin geçici olarak kararsız hale gelmesine ve erişilebilirliğin azalmasına yol açabileceğini söylediler. Yuan ve arkadaşları [14], Raft algoritmasındaki tutarlılık problemini Lider Seçimi, Log Replikasyonu ve Güvenlik olarak üç bağımsız alt probleme bölmüşlerdir. Oyinloye ve arkadaşları [15], ana akım protokollerinin bahsedilen hala dezavantajlarına yönelik bu protokollerini geliştirme çabaları neticesinde, tıp veya ulaşım gibi belirli alanlara hitap eden alternatif fikir birliği protokollerinin doğmasına yol açtığını vurgulamışlardır. Bu alternatif protokollerin, araştırılmaya değer özgün özellikler

barındırmalarına rağmen, genel olarak yeterince tanınmadıklarını belirtmişlerdir.

II. MATERYAL VE METOT

Alternatif konsensüs algoritmaları, çeşitli konsensüs algoritmalarının performans olarak negatif özelliklerini iyileştirmek üzerine mevcut konsensüs algoritmaları üzerindeki iyileştirmeleri hedef olarak ortaya çıkmaktadır. RAFT protokolünün düğüm sayısı fazla olan ağlardaki performans düşüklüğü veya Bizans düğümlerine tahammül edememesi gibi iyileştirilebilecek durumların olması, alternatif konsensüslerin ortaya çıkmasına sebep olmaktadır. Banor ve arkadaşları [16], fikir birliği protokol algoritmalarının önemli bileşenlerini tartıştılar ve bunları performans, güvenlik özellikleri açısından analiz edip değerlendirmişlerdir. Alsunaidi ve arkadaşları [17], fikir birliği protokol algoritmaları hakkında bir anket çalışması yaptılar ve güçlü ve zayıf yanlarını karşılaştırmalı şekilde sınıflandırmışlardır. Bu bölümde RAFT algoritmasının eksik yanları üzerinde yapılan çalışmalar sonucu ortaya çıkan RR-RAFT, LRD-RAFT, X-RAFT, RE-RAFT algoritmalarının gecikme ve verim metrikleri baz alınarak, karşılaştırmalı olarak performans analizlerinin yapılması amaçlanmaktadır.

A. Konsensüs Algoritmaları

1) RAFT Algoritması

Liu ve arkadaşları [18], Raft protokolünü öne çıkaran temel özelliğinin, Paxos'a kıyasla çok daha basit bir yapıya sahip olduğunu ifade etmişlerdir. Algoritmanın çalışma prensibi ile ilgili, mesajların tutarlılığı, bir lider seçimiyle sağlandığını ve bu durum Raft algoritmasını lider odaklı bir yapı haline getirdiğini belirttiler. Ancak, lider düğümünde bir sorun meydana geldiğinde, yeni bir lider belirlenmesi gerektiğini; bu süreç zahmetli olup fikir birliğine ulaşma hızını düşürebileceğini söylediler. Raft algoritmasının, bir düğümün kötü niyetli hareketlerini tespit etme ve engelleme yeteneğine sahip olmadığını belirttiler.

2) LRD-RAFT Algoritması

Yang ve arkadaşları [19], LRD-Raft algoritmasını tanıtarak, klasik Raft'ta sadece liderin sorumlu olduğu kayıt çoğaltma yükünü takipçi (follower) düğümlere de devrederek dağıttılar. Bu iyileştirme ile, lider üzerindeki yükün azalmasını sağlayarak, yüksek TPS (transaction per second) değerine ulaşabildiklerini vurgulamışlardır.

LRD-Raft algoritmasındaki her bir takipçi düğüm, kendi bağımsız DLog'unu (Ayrık Kayıt) tutar, istemciden gelen istekleri alır ve bu kayıtları çoğaltır. Takipçi tarafından çoğaltılan DLog, lider düğüm tarafından TagEntry aracılığıyla doğrulanır ve ardından durum makinesine uygulanır. Bu yöntem, liderin yetkisini azaltmadan kayıt çoğaltma yükünü sistem genelinde dağıtır. Tablo 1'de Lrd-Raft algoritması için kullanılan terimler bulunmaktadır.

Tablo 1. Lrd-Raft Terimleri

Değer	Anlamı
Dlog	Takipçi düğümler tarafından tutulan ayrık kayıtlar.
DEntry	Takipçi düğümler tarafından oluşturulan DLog içindeki giriş.
TagEntry	NormalLog içindeki ve bir DEntry'e işaret eden, veri içermeyen giriş.

NormalLog	Lider düğüm tarafından tutulan kayıt.
NormalEntry	Lider düğüm tarafından oluşturulan NormalLog içindeki giriş.
weakCommitState	DEntry, çoğunluk düğümlere ve lidere çoğaltıldığında weakCommitState durumuna girer.
strongCommitState	Lider düğüm, TagEntry'yi çoğunluk düğümlere çoğalttığında ilgili DEntry, strongCommitState durumuna girer.

3) RR-RAFT Algoritması

Li ve arkadaşları [20], RR-RAFT algoritması ile birlikte, regresyon algoritmasına dayanan bir itibar değerlendirme modeli önererek, düğümlerin itibarını daha doğru bir şekilde değerlendirmek için orijinal lojistik regresyon algoritmasına dayalı bir itibar ölçüm fonksiyonu ve bir itibar tüketim fonksiyonu tanıtmışlardır ve ağın başlangıcında ortaya çıkabilecek itibar yoğunlaşması sorununu önlemek için itibar artış hızını makul bir itibar tüketim mekanizmasıyla kontrol eder ve hızlı bir lider düğüm seçim stratejisi sağlayarak Raft algoritmasının uzlaşma verimliliğini artırmayı hedeflemişlerdir.

RR-RAFT algoritması düşük gecikme, yüksek güvenlik ve yüksek verimliliği aynı anda sağlayamayan mevcut Raft algoritmalarının eksikliklerini çözmek için algoritmada 3 ana faz uygulamaktadır. Bu fazlar; itibar modeli oluşturma fazı, lider seçim fazı, kayıt çoğaltma fazıdır.

4) X-RAFT Algoritması

Li ve arkadaşları [21], X-RAFT algoritması ile birlikte, lider seçimini ve kayıt çoğaltmayı geliştirmek ve kayıt tutarlılığını ve sistem sürdürülebilirliğini bir canlılık sıfırlama mekanizması oluşturarak Bizans hatası olasılığını düşürmeyi amaçlamaktadır ve RAFT algoritmasından daha güvenli bir yapı haline gelmesini hedeflemişlerdir.

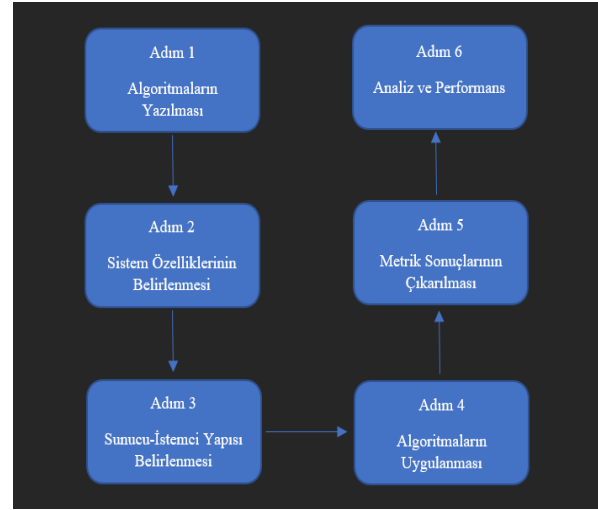
X-RAFT algoritması RAFT algoritmasını temel alır ve modüler yapısını koruyarak, ölçeklenebilirlik ile verimlilik sorunlarına yönelik çözümler sunar. X-RAFT algoritması; lider, takipçi, aday ve monitör olmak üzere dört rolden oluşur. RAFT'tan farklı olarak, sisteme monitör rolü eklenmiştir. Monitörler, liderin hareketlerini denetler ve eğer lider kötü niyetli davranış sergilerse, en yüksek vitality puanına sahip monitör doğrudan yeni lider olarak atanır.

5) RE-RAFT Algoritması

Wang ve arkadaşları [22], RE-RAFT algoritmasını geliştirerek, ağdaki liderlerin illegal olarak değiştirilmesi sorunun çözümü için, bir çökme toleransı sistemi ve gelişmiş Bizans direnci özelliklerini Raft algoritmasına ekleyerek güvenli bir konsensüs algoritması önermişlerdir.

B. Deney Ortamı

Yapılacak çalışmada, Raft algoritması tabanlı alternatif konsensüs algoritmalarının analizi, gRPC çerçevesi kullanılarak bir blokzincir simülasyon uygulaması içerisinde, performansları karşılaştırmalı olarak analiz edilecektir. İşlem hacmi (throughput) deneyleri ve konsensüs gecikmesi deneyleriyle performans sonuçlarının karşılaştırılması amaçlanmaktadır. Bu amaçla oluşturulacak çalışma adımları Şekil 1'de belirtilmiştir.



Şekil 1. Çalışma Adımları

1) İşlem Hacmi (Throughput)

Ouattara ve arkadaşlarına göre işlem hacmi veya verimlilik [23], blokzincir sistemlerinde birim zaman içinde doğrulanan ve ağ üzerinde dağıtılan blok sayısını ifade eder. Bu metrik, genellikle saniye başına işlem sayısı (Transactions per second -Tps) olarak ifade edilir ve sistemin bir saniyede işleyebildiği toplam işlem miktarını gösterir. Blokzincirlerde verimlilik metriği, genellikle saniyede oluşturulan blok sayısı olarak ölçülmektedir.

2) Gecikme (Latency)

Yuan, Haotian ve arkadaşlarına göre gecikme [24], bir işlemin onaylanması ile ağa iletilmesi arasındaki süre farkının, toplam işlem sayısına oranlanmasıyla hesaplanır. Bu çalışmada ortalama gecikme metriği, blokların oluşturulmasından başlayarak, zincire yazılmasına kadar geçen süre olarak hesaplanacaktır.

C. Simülasyon Özellikleri

Simülasyon, istemci-sunucu mimarisi ile oluşturulacaktır. Tasarlanacak simülasyonda kullanılacak giriş verileri, gerçek verilerden oluşan blokzincir veri setleri kullanılarak oluşturulması hedeflenmektedir. Simülasyonda kullanılacak İstemci-sunucu mimarisi, gRPC çerçevesi kullanılarak oluşturulacaktır. gRPC çerçevesi [25], Her ortamda çalışabilen, modern, açık kaynaklı ve yüksek performanslı bir Uzaktan Prosedür Çağrısı (RPC) çerçevesidir. Veri merkezleri arasında ve içinde hizmetleri etkili şekilde birbirine bağlayabilir; yük dengeleme, gözlemleme, sağlık durumu takibi ve kimlik doğrulama gibi işlevler için genişletilebilir desteğe sahiptir. Simülasyonda düğüm sayısı, algoritma özellikleri ve işlemci çekirdek sayısına göre, gecikme ve verim metrikleri üzerinden performans analizi gerçekleştirilecektir. Simülasyonda gerçekçi bir ağ davranışı görmek için mesaj iletimi işleminde rastgele veya gerçek verilerden oluşan blokzincir veri setlerinden gecikme (delay) ve paket kaybı (loss) işlemleri simülasyona verilecektir. Simülasyonda gRPC protokolü kullanılacaktır. Her algoritma için lider seçimi işlemi ve blok oluşturulup, düğümlere iletme işlemleri, belirli sayıda turlarla gerçekleştirilecektir. Simülasyondaki her düğüm, bir docker konteyner olarak çalışacaktır. Bu işlemler sonucunda gecikme ve verim metriklerinin ortalaması alınarak sonuç elde edilmesi planlanmaktadır. Simülasyonun

çalıştırılacağı sistem özellikleri Tablo 2’de, simülasyon girdileri Tablo 3’te belirtilmiştir.

Tablo 2. Sistem Özellikleri

Parametre	Değer
Cpu	Intel i7 6700HQ 2.6 GHz
Ram	32 GB
Çekirdek Sayısı	4

Tablo 3. Simülasyon Özellikleri

Düğüm Sayısı	8-16-24-32
Protokol	gRPC
Programlama dili	Python

III. SONUÇLAR

Liu ve arkadaşları [26], alternatif fikir birliği protokollerinin henüz gelişiminin erken aşamalarında olsa da ölçeklenebilirlik, enerji verimliliği ve güvenlik gibi temel sorunlara yönelik yenilikçi çözümler sunmakta olduğunu vurgulamaktadır. Bu çalışmada test edilecek alternatif konsensüs algoritmalarının performans sonuçları ile birlikte, bir blokzincir ağı simülasyonu üzerinde Raft algoritması ve alternatif konsensüs algoritmalarının karşılaştırmalarının yapılması planlanmaktadır. Ortaya çıkacak performans sonuçları, seçilen Raft algoritması tabanlı konsensüs algoritmalarının, bu algoritmaların kullanılması planlanan bir blokzincir üzerindeki performansları üzerine fikir vermesi amaçlanmaktadır. Alternatif konsensüs algoritmalarından RE-RAFT algoritması, çok düğümlü zincirlerde (örneğin bir bankanın tüm şubelerindeki müşterilerin para transferlerinin bulunduğu bir zincir), ağ verimlilik performansının yüksek olması beklenmektedir. LRD-RAFT algoritmasında lider üzerindeki yük azaldığı için sistem, yüksek TPS (transaction per second) değerine ulaşılması beklenmektedir. X-RAFT algoritması EdgeAI-Human-IoT sistemleri için RAFT’e göre çok daha güvenli bir yapı sunmayı amaçlamaktadır. Bunun yanında RR-RAFT algoritması, Raft algoritmasına göre daha az sayıda düğüm olan zincirlerde yüksek performans göstermektedir. Örneğin, kaynak kullanımı ve sayıca az düğüm olan IoT ağlarında RR-Raft algoritmasının kullanımı ağ performansı açısından daha öngörülebilirdir. Tablo 4’te RR-Raft algoritmasının 5 düğümlü bir ağdaki performansının örnek gösterimi bulunmaktadır. Verim metriği, RR-Raft algoritmasında, lider düğümün kayıtları diğer düğümlere iletmesi ve başarılı blokların 1 saniyede eklenme işlemi olarak öne çıkmaktadır. Ağdaki gecikme, 5 düğüm için yaklaşık 3ms olmasına rağmen düğüm sayısının artmasıyla birlikte ağdaki gecikmenin artması beklenmektedir.

Tablo 4. RR-Raft Algoritmasının Örnek Performans Test Sonuçları

Parametre	Değer	Anlamı
Tur Sayısı	50	50 ayrı turda (term’de) bir lider aday seçildi
Verim	353.67	Saniyede ~354 başarılı “append” işlemi
Ortalama Gecikme	2.3 ms	ortalama gecikme <3 ms seviyesinde

IV. TARTIŞMA

Her algoritmanın farklı senaryolarda güçlü ve zayıf yönleri mevcuttur. Bu farklılıklar, algoritmaların tasarım önceliklerinden ve hedefledikleri sistem gereksinimlerinden

kaynaklanmaktadır. Her algoritmanın tercih edilme sebebi, uygulamanın performans, güvenlik ve ölçeklenebilirlik beklentilerine göre değişkenlik göstermektedir. Simülasyon ortamı, gerçek ağ davranışlarını tam anlamıyla taşımamaktadır. Sonraki çalışmalarda gerçek ağ davranışlarının da teste dahil edildiği bir simülasyon ortamı sağlanacaktır.

REFERANSLAR

- [1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” Cryptography Mailing List, <https://metzdowd.com>, Mar. 24, 2009. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [2] R. Beck, J. Stenum Czepluch, N. Lollike, and others, “Blockchain – The gateway to trust-free cryptographic transactions,” in Proc. 24th European Conference on Information Systems (ECIS), Istanbul, Turkey, 2016, pp. 1–14.
- [3] S. Abeyratne and R. Monfared, “Blockchain ready manufacturing supply chain using distributed ledger,” International Journal of Research in Engineering Technology, vol. 5, Sep. 2016.
- [4] ITU-T Focus Group on Application of Distributed Ledger Technology, “Distributed ledger technology security framework,” ITU, 2019. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/dl1.pdf>.
- [5] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Communications Surveys & Tutorials vol.: 18, Issue: 3, pp. 2084-2123, thirdquarter 2016.
- [6] N. Alzahrani and N. Bulusu, “Towards true decentralization: A blockchain consensus protocol based on game theory and randomness,” in Proc. 9th Int. Conf. Decision and Game Theory for Security GameSec, Seattle, WA, USA, Oct. 29–31, 2018, pp. 465–485.
- [7] S. Hattab and I. Alyaseen, “Consensus algorithms blockchain: A comparative study,” in International Journal on Perceptive and Cognitive Computing, vol. 5, pp. 66–71, Dec. 2019.
- [8] T. Nguyen and K. Kim, “A survey about consensus algorithms used in blockchain,” in Journal of Information Processing Systems, vol. 14, pp. 101–128, Jan. 2018.
- [9] W. Wang et al., “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” in IEEE Access, vol. 7, pp. 22328-22370, 2019.
- [10] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564.
- [11] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” in Association for Computing Machinery, vol. 4, no. 3, pp. 382–401, Jul. 1982.
- [12] L. Ni, Q. Ye, J. Yang, S. Zhang and M. Xian, “Research of Raft Algorithm Improvement in Blockchain,” 2024 IEEE 16th International Conference on Advanced Infocomm Technology (ICAIT), Enshi, China, 2024, pp. 290-294.
- [13] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference, Philadelphia, PA, USA, 2014, pp. 305–320.
- [14] Y. Yuan, “Blockchain: The state of the art and future trends,” Acta Automatica Sinica, vol. 42, pp. 481–494, Apr. 2016.
- [15] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, “Blockchain consensus: An overview of alternative protocols,” in Symmetry, vol. 13, no. 8, p. 1363, 2021.
- [16] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, “SoK: Consensus in the age of blockchains,” in Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, 2019, pp. 183–198.
- [17] S. J. Alsunaidi and F. A. Alhaidari, “A Survey of Consensus Algorithms for Blockchain Technology,” in 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-6.
- [18] X. Liu and W. Yu, “A Review of Research on Blockchain Consensus Mechanisms and Algorithms,” 2024 9th International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, Japan, 2024, pp. 1-10.
- [19] H. Yang, Y. Feng and W. Zhang, “LRD-Raft: Log Replication Decouple for Efficient and Secure Consensus in Consortium-Blockchain-Based IoT,” in IEEE Internet of Things Journal, vol. 12, no. 7, pp. 8807-8820, 1 April, 2025.

- [20] S. Li, X. Deng and Y. Zou, "RR-Raft: A Raft Consensus Algorithm Based on Reputation Regression Model and RSA Signature," 2024 2nd International Conference On Mobile Internet, Cloud Computing and Information Security (MICCIS), Changsha City, China, 2024, pp. 92-96.
- [21] F. Li, J. Wang, W. Xie, N. Tong and D. Wang, "X-RAFT: Improve RAFT Consensus to Make Blockchain Better Secure EdgeAI-Human-IoT Data," in *IEEE Transactions on Emerging Topics in Computing*, vol. 13, no. 1, pp. 22-33, Jan.-March 2025.
- [22] Z. Wang, C. Xu, S. Dai and X. Li, "Re-Raft: An Improved Blockchain Consensus Algorithm with Enhanced Byzantine Resistance and Crash Tolerance," 2024 2nd International Conference on Computer, Vision and Intelligent Technology (ICCVIT), Huaibei, China, 2024, pp. 1-6.
- [23] H. F. Ouattara, D. Ahmat, F. T. Ouédraogo, T. F. Bissyandé, and O. Sié, "Blockchain consensus protocols," in *Proc. AFRICOMM 2017 – e-Infrastructure and e-Services for Developing Countries**, V. Odumuyiwa, O. Adegboyega, and C. Uwadia, Eds., Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 250. Cham, Switzerland: Springer, 2018.
- [24] H. Yuan, F. Li, R. Diao, and T. Shu, "Double-layer Byzantine fault-tolerant grouping consensus algorithm based on Raft," in *IET Blockchain*, vol. 4, pp. 555–569, Apr. 2024.
- [25] gRPC Authors, "gRPC: A high-performance, open-source universal RPC framework," gRPC.io. [Online]. Available: <https://grpc.io>.
- [26] X. Liu and W. Yu, "A Review of Research on Blockchain Consensus Mechanisms and Algorithms," 2024 9th International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, Japan, 2024, pp. 1-10.