ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№4
2025

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

4 (356)

OCTOBER – DECEMBER 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

МАЗМҰНЫ

СОДЕРЖАНИЕ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 4. Namber 356 (2025).102–121

https://doi.org/10.32014/2025.2518-1726.386

UDC 004.056.2

©A.Sh. Barakova[1,2], K.S. Shadinova[1], A.S. Orynbaeva[3], G. Sugurzhanova[4], 2025.
[1] Asfendiyarov Kazakh National Medical University, Almaty, Kazakhstan;
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[3]Astana Medical University, Astana, Kazakhstan;
[4]NEI «Kazakhstan-Russian Medical University», Almaty, Kazakhstan.
E-mail: balia_79@mail.ru

DESIGN OF A MODEL FOR PROTECTING A WEBSITE'S AUTHENTICATION DATA AND CONTENT BASED ON BLOCKCHAIN TECHNOLOGY

Barakova Aliya — Assistant Professor of the Department of Engineering Disciplines and Good Practices, Asfendiyarov Kazakh National Medical University; doctoral student of Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: balia_79@mail.ru, https://orcid.org/0000-0002-0904-745X;
Shadinova Kunsulu — Associate Professor Shadinova Kunsulu Seidazovna Kazakh National Medical University named after Asfendiyarov, Almaty, Kazakhstan,
E-mail: Shadinkunsulu@gmail.com; https://orcid.org/0009-0006-5534-7927;
Orynbayeva Ainur — senior lecturer at Astana Medical University. Astana, Kazakhstan,
E-mail: ainur_tas@mail.ru, https://orcid.org/0009-0005-4984-281X;
Sugurzhanova Gulzhan — Senior Lecturer of the Department of Social Sciences, NEI «Kazakhstan-Russian Medical University», Almaty, Kazakhstan,
E-mail: sugurzhanova83@mail.ru, https://orcid.org/0000-0001-8334-6856.

Abstract. The article introduces a new PBFT-based consensus algorithm designed to enhance the scalability, reliability, and security of consortium blockchain systems. The approach is implemented within a four-layer architecture—network, consensus, application, and meta-application—and relies on segmenting nodes into three functional groups. Proxy nodes perform local consensus, global proxy nodes aggregate blocks across segments, while supernodes supervise system-wide operations and ensure reliability. The algorithm incorporates guarantee mechanisms, trusted node selection, and dual-leader monitoring to strengthen fault tolerance and mitigate malicious behavior. Theoretical and experimental evaluations confirm the efficiency of the segmented consensus structure. The required number of nodes decreases from 3f+1 to 2f+1, improving resource utilization. Consensus latency ranges from 80 to 147 ms, demonstrating a 62–70% improvement compared to classical PBFT. Communication complexity is optimized to the O(n)–O(n²) range.

Simulations conducted in Python, with visualization through Matplotlib, validate the performance model. The algorithm was implemented in a working prototype: content hashing and IPFS integration were developed in Python, while a Solidity smart contract records ownership metadata, hash values, and IPFS CIDs. The prototype, deployed on the *www.AliyaSchool.kz* platform and tested under real conditions, confirmed the correct execution of the smart contract via Remix IDE. Overall, the proposed PBFT-based algorithm provides an effective solution to the blockchain scalability problem, enabling distributed load handling, accelerated consensus, and improved detection of malicious nodes. The work contributes a scientifically grounded model to the national research base and offers methodological value for further development of secure blockchain mechanisms for web systems.

Keywords: blockchain, consensus algorithm, scalability, security, PBFT, smart contract, IPFS

© А.Ш. Баракова,[1,2], К.С. Шадинова[1], А.С. Орынбаева[3], Г. Сугуржанова[4], 2025.

[1] С. Асфендияров Атындағы Қазақ ұлттық медицина университеті, Алматы, Қазақстан;

[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;

[3]Астана медицина университеті, Астана, Қазақстан;

[4]Қазақстан-Ресей медициналық университет, Алматы, Қазақстан.
E-mail: balia_79@mail.ru

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ НЕГІЗІНДЕ ВЕБ САЙТТЫҢ АУТЕНТИФИКАЦИЯЛЫҚ ДЕРЕКТЕРІ МЕН ӨНІМІН ҚОРҒАУ МОДЕЛІН ҚҰРАСТЫРУ

Баракова Алия — профессор ассистент, С.Ж. Асфендияров атындағы Қазақ ұлттық медицина университеті; Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, Алматы, Қазақстан,
E-mail: balia_79@mail.ru, https://orcid.org/0000-0002-0904-745X;
Шадинова Күнсұлу — қауымдастырылған профессор, С.Ж. Асфендияров атындағы Қазақ ұлттық медицина университеті, Алматы, Қазақстан,
E-mail: Shadinkunsulu@gmail.com, https://orcid.org/0009-0006-5534-7927;
Орынбаева Айнұр — Астана медицина университетінің аға оқытушысы, Астана, Қазақстан,
E-mail: ainur_tas@mail.ru, https://orcid.org/0009-0005-4984-281X;
Сугуржанова Гүлжан — «Қазақстан-Ресей медициналық университеті» Әлеуметтік ғылымдар кафедрасының аға оқытушысы, Алматы, Қазақстан,
E-mail: sugurzhanova83@mail.ru, https://orcid.org/0000-0001-8334-6856.

Аннотация. Бұл мақала консорциумдық блокчейн жүйелерінің ауқымдылығын, сенімділігін және қауіпсіздігін арттыруға бағытталған PBFT негізіндегі жаңа консенсус алгоритмін таныстырады. Тұғыр төрт деңгейлі архитектураға негізделген: желілік, консенсус, қолданбалық және мета-қолданбалық. Жүйе түйіндерді үш функционалдық топқа сегменттеу

арқылы жұмыс істейді. Прокси түйіндер жергілікті консенсусты орындайды, жаһандық прокси түйіндер сегменттер арасынан блоктарды біріктіреді, ал супернода жүйе жұмысын жалпы бақылауды қамтамасыз етеді. Алгоритмде кепілдік механизмдері, сенімді түйіндерді таңдау стратегиясы және қос көшбасшыны бақылау тәсілі қолданылып, ақауларға төзімділік күшейтіледі және зиянды әрекеттердің алдын алады. Теориялық және тәжірибелік бағалау сегменттелген консенсус құрылымының тиімділігін дәлелдейді. Қажетті түйіндер саны 3f+1-ден 2f+1-ге дейін азайып, ресурстарды пайдалану жақсарады. Консенсус кідірісі 80–147 мс аралығында болып, дәстүрлі PBFT-тен 62–70 процент жылдамырақ нәтижені көрсетеді. Байланыс күрделілігі O(n)–O(n²) ауқымында оңтайландырылды. Python тіліндегі модельдеу және Matplotlib визуализациясы алгоритмнің өнімділігін растады. Алгоритмнің жұмыс прототипі жүзеге асырылды: контент хештеу және IPFS-пен интеграция Python арқылы орындалды, ал Solidity тіліндегі смарт-келісім контент иесін, хеш мәнін және IPFS CID-ін тіркейді. *www.AliyaSchool.kz* платформасында сынақтан өткізілген прототип Remix IDE арқылы смарт-келісімнің дұрыс орындалуын дәлелдеді. Жалпы алғанда, ұсынылған PBFT негізіндегі алгоритм блокчейннің ауқымдылық мәселесін тиімді шешіп, жүктемені бөлуді, консенсусты жылдамдатуды және зиянды түйіндерді анықтауды қамтамасыз етеді. Бұл жұмыс ұлттық ғылыми базаға үлес қосып, веб-жүйелерге арналған қауіпсіз блокчейн механизмдерін дамытуға әдістемелік негіз ұсынады.

Түйін сөздер: блокчейн, консенсус алгоритмі, масштабталу, қауіпсіздік, PBFT, смарт-контракт, IPFS

© А.Ш. Баракова[1,2], К.С. Шадинова[1], А.С. Орынбаева[3], Г. Сугуржанова[4], 2025.

[1]Казахский национальный медицинский университет имени С.Д. Асфендиярова, Алматы, Казахстан;

[2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;

[3]Медицинский университет Астана, Астана, Казахстан;

[4]НЕИ «Казахстанско-Российский медицинский университет, Алматы, Казахстан.

E-mail: balia_79@mail.ru

РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ И КОНТЕНТА ВЕБ-САЙТА НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Баракова Алия — ассистент профессора, Казахский национальный медицинский университет имени С.Д. Асфендиярова; докторант Казахского национального университета имени аль-Фараби, Алматы, Казахстан,
E-mail: balia_79@mail.ru, https://orcid.org/0000-0002-0904-745X;

Шадинова Күнсулу — доцент Казахского национального медицинского университета имени С.Д. Асфендиярова, Алматы, Казахстан,
E-mail: Shadinkunsulu@gmail.com, https://orcid.org/0009-0006-5534-7927;
Орынбаева Айнур — старший преподаватель Астанинского медицинского университета, Астана, Казахстан,
E-mail: ainur_tas@mail.ru, https://orcid.org/0009-0005-4984-281X;
Сугуржанова Гулжан — старший преподаватель кафедры социальных наук НЕИ «Казахстанско-Российский медицинский университет», Алматы, Казахстан,
E-mail: sugurzhanova83@mail.ru, https://orcid.org/0000-0001-8334-6856.

Аннотация. В данной статье представлен новый консенсусный алгоритм на основе PBFT, направленный на повышение масштабируемости, надежности и безопасности консорциумных блокчейн-систем. Подход реализован в четырехуровневой архитектуре: сетевом, консенсусном, прикладном и мета-прикладном уровнях. Работа системы основана на сегментации узлов на три функциональные группы. Прокси-узлы выполняют локальный консенсус, глобальные прокси-узлы агрегируют блоки между сегментами, а суперузлы обеспечивают общее системное наблюдение. Алгоритм дополняется механизмами гарантий, стратегией выбора доверенных узлов и контролем двух лидеров, что усиливает устойчивость к сбоям и снижает риски вредоносного поведения. Теоретическая и экспериментальная оценка подтверждает эффективность сегментированной архитектуры консенсуса. Количество необходимых узлов снижается с 3f+1 до 2f+1, что улучшает использование ресурсов. Задержка консенсуса составляет 80–147 мс и демонстрирует ускорение на 62–70% по сравнению с классическим PBFT. Сложность коммуникаций оптимизирована в диапазоне от O(n) до $O(n^2)$. Моделирование, выполненное на Python с визуализацией в Matplotlib, подтвердило работоспособность модели. Алгоритм был реализован в виде рабочего прототипа: хеширование контента и интеграция с IPFS выполнены на Python, а смарт-контракт на Solidity регистрирует владельца контента, хеш и IPFS CID. Прототип, протестированный в реальных условиях на платформе *www.AliyaSchool.kz*, подтвердил корректное выполнение смарт-контракта через Remix IDE. В целом, предложенный алгоритм на основе PBFT эффективно решает проблему масштабируемости блокчейна, обеспечивает распределение нагрузки, ускоренный консенсус и улучшенное обнаружение вредоносных узлов. Работа формирует научно обоснованную модель и служит методологической базой для дальнейшего развития защищенных блокчейн-механизмов для веб-систем.

Ключевые слова: блокчейн, консенсусный алгоритм, масштабируемость, безопасность, PBFT, смарт-контракт, IPFS

Кіріспе. Бүкіл әлемдегі инфрақұрылымның маңызды салаларына кибершабуылдар саны жыл сайын тұрақты өсіп келеді. Қазіргі заманғы ақпараттық жүйелердің басым көпшілігі веб-сайттар ретінде құрылады,

сондықтан қауіпсіздікке ерекше назар аудару қажет. Яғни кез- келген операциялық жүйесі мен бағдарламалық қосымшасы бар құрылғы пайда болған соң, ол бірден тәртіп бұзушылардың қызығушылығын тудырады. Олар оны зерттей бастайды және оны бұзуға күш жұмсайды. Бүгінгі күні веб-сервистерді қорғау барлық ұйымдарды алаңдатады, себебі қасақана субъектілер оны рұқсатсыз пайдалану мақсатында жеке немесе заңды тұлға туралы кез келген ақпаратты алуға ұмтылады.

Әлемдік және отандық экономиканы трансформациялаудың қазіргі кезеңі коммерциялық қызмет пен цифрлық технологиялар арасындағы интеграциялық процестерді күшейтуге ықпал етеді, олардың соңғысы бизнес субъектілерінің қарқынды дамуының басты факторы болып табылады.

Әдебиеттерге шолу. Шетелдік ғалымдар Huynh T. және әріптестері (Huynh et al, 2019) блокчейн технологиясының қауіпсіздігі мен құпиялылығы бойынша жан-жақты шолу жасап, кең таралған шабуыл түрлерін сипаттап, олардан қорғану жолдарын ұсынады.

X. Li және авторлар тобы (Li et al, 2020) блокчейн жүйелеріне бағытталған шынайы шабуылдар мен қауіп-қатерлерді жүйелі түрде талдап, олардың негізінде қауіпсіздік мәселелерінің ауқымын сипаттайды. Олар қазіргі заманғы блокчейн инфрақұрылымдарының осал тұстарын ашып көрсетіп, шабуылдардың техникалық ерекшеліктеріне терең тоқталады

Басқа бір маңызды үлес – J. Leng және авторлар ұсынған (Leng et al, 2022) PDI (Process-Data-Infrastructure) моделі. Бұл үлгі блокчейн қауіпсіздігі мәселелерін үш негізгі деңгейде – процесс, дерек, және инфрақұрылым деңгейінде жіктеп, талдау жасауға мүмкіндік береді. Зерттеушілер техникалық зерттеулер мен бизнес міндеттер арасындағы алшақтықты жоюға тырысып, қауіпсіздік проблемаларын жүйелі түрде шешудің жолдарын іздейді.

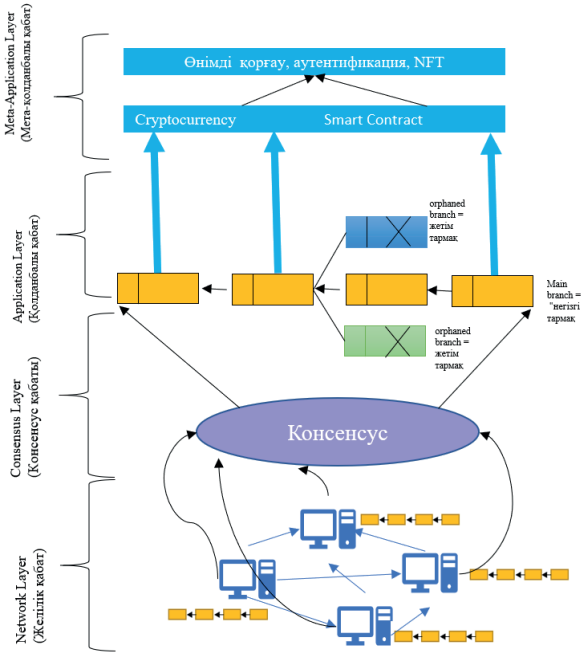
Әдістер мен материалдар. Бұл зерттеу жұмыста ақпараттарды қорғаудың тиімді тәсілін ұсыну. Ақпаратты қорғаудың қазіргі таңда көп мөлшерде түрлері көп. Соңғы заманауи технолгиялардың бірі блокчейн технологиясы зерттеу жұмыстың өзегі болып табылады. Блокчейн технологиясы мінсіз әрі сенімді технология ретінде өте танымал. Дегенмен оның да кемшіл тұстары бар. Блокчейн технолгиясының ең басты кемшіліктерінің бірі транзакция жылдамдығы мен масштабталу мәселесі болып табылады (Bonneau et al, 2015).

Масштабталу мәселесін шешуге арналған жаңа консенсус алгоритмін әзірлеу мақаланың негізгі кілті. Пайдаланушыларды жылдам әрі қауіпсіз аутентификациялау және веб-контентті сенімді қорғау үшін масштабталатын және тиімді консенсус алгоритмі қажет. Мәселенің шешімі ретінде жаңа консенсус механизмін құрастыру керек. Зерттеу жұмыста сегменттеуге негізделген PBFT негізіндее құрылған жаңа консенсус алгоритмы ұсынылады, ол консорциумдық блокчейннің орталықсыздандыру, қауіпсіздік және масштаблауы талаптарына сай болуын қамтамасыз етуге бағытталған (Popadyuk et al, 2020, Sompolinsky et al, 2016).

PBFT негізінде құрылған жаңа алгоритмін құру үшін 1 - суретте блокчейн жүйесінің архитектурасын төрт негізгі қабат бойынша сипаттайды: желілік қабат (түйіндер арасындағы байланыс), консенсус қабаты (шешімге келу үдерісі), қолданбалы қабат (криптовалюта және смарт-келісімшарттар), және мета-қолданбалы қабат (өнімді қорғау, аутентификация және NFT). Әр қабат өзіне тән міндеттерді атқара отырып, жүйенің қауіпсіздігін, тұрақтылығын және масштабталуын қамтамасыз етеді. Жаңа алгоритмді құру осы төрт кезеңнің үйлесімділігін ескере отырып, блокчейн технологиясын онлайн контентті қорғау мақсатында тиімді пайдаланылады.

Жаңа консенус алгоритмі PBFT негізінде құрылады. Себебі PBFT алоритмі BFT алгоритмінің төмен тиімділігі мәселесін шешеді, ал коммуникацияның күрделілігі экспоненциалдыдан көпмүшелікке өзгереді (Somin et al, 2018).

Блокчейн архитектурасының негізінде жатқан консенсус қауіпсіздік, тиімділік және масштабталуды оңтайландыру тұрғысынан сервистік бағдарланған қосымшаларды жүзеге асырудың кілті болып табылады. Консенсус алгоритмдерінің кейбір күрделі түрлерінде, мысалы, Practical Byzantine Fault Tolerance (PBFT), желідегі түйіндер саны артқан сайын өткізу қабілеті күрт төмендейді. Ал қарапайым алгоритмдерде, мысалы, Raft жүйесінде, желі көлемі ұлғайған сайын жетекшіге түсетін жүктеме артып, консенсус тиімділігіне теріс әсер етеді. Осы мәселелерді шешу үшін біз консорциумдық блокчейн негізінде сенімділік ағашына сүйенген түйіндер сегменттерінің моделін ұсынамыз.



Сурет 1- Алгоритм кезеңдері

Бұл модель жоғары масштабталуды белгілі бір деңгейдегі орталықсыздандыру мен қауіпсіздікті сақтай отырып қамтамасыз етеді.

Біріншіден, біз түйіндер арасындағы сенімділік қатынастарын бейнелейтін кепілдік механизмін құрамыз, содан кейін осы механизм негізінде түйіндерді таңдау стратегиясын әзірлейміз. Бұл стратегия түйіндердің кепілдік нәтижелерін және консенсус әрекетін бағалап, сенімділік мәртебесін анықтап, зиянды түйіндерді анықтап, сенімді көшбасшылар тізімін жасақтайды. Екіншіден, біз қос көшбасшы бақылау механизмін ұсынамыз, онда резервтік көшбасшы негізгі көшбасшының белсенділігін бақылап отырады, ал оның белсенділігі консенсус түйіндерімен бағаланады.

Жаңа PBFT негізінде құрылған алгоритм алдымен кластерлеу алгоритмын қолданып, желідегі түйіндерді аралас атрибуттарына сәйкес сегменттерге бөледі. Сегменттеу технологиясы алғаш рет дерекқорларды бөліктерге бөлу үшін қолданылған. Бұл технология үлкен дерекқорларды басқаруға ыңғайлы, жылдам және кіші бөліктерге бөлуге мүмкіндік береді. Блокчейнге қатысты сегменттеу технологиясы үш түрге бөлінеді: желіні сегменттеу, транзакцияны сегменттеу және күйді сегменттеу. Elastico20 протоколы — блокчейн консенсус алгоритмінде сегменттеу технологиясын алғаш қолданған протокол. Алайда бұл протокол ашық блокчейнге арналғандықтан, түйіндерді тексеруге ынталандыру үшін экономикалық стимулдарды қажет етеді, сондықтан консорциумдық желіге жарамайды.

Содан кейін, әртүрлі сегменттерде параллельді консенсусқа қол жеткізу үшін қиылысатын емес транзакциялар пайдаланылды. Сегмент өлшемін таңдау биномдық ықтималдықтар үлестірімі арқылы талданады, сондай-ақ әртүрлі түйіндердің істен шығу ықтималдығына байланысты жүйенің жаһандық блокты сәтті қалыптастыру мүмкіндігі зерттелді. Желілік өзара әрекеттестік — бұл сенімді тең дәрежелі (peer-to-peer) желі. Келісілген шешімдер қабылдайтын түйіндер басқа түйіндерден хабарламалар ала алады. Кең тарату (broadcast) хабарламалары жіберушіні желідегі барлық түйіндерге, соның ішінде өзіне де хабарлама жіберуге мәжбүрлейді (Баракова et al, 2022).

Бұл жұмыста жартылай синхронды (semi-synchronous) желілік модель пайдаланылады. Хабарламаны жіберу уақытының жоғарғы шегі белгіленеді – бұл хабарламаның жіберілуі мен қабылдануы арасындағы уақыт аралығы. Егер жіберу уақыты осы шектен асып кетсе, хабарлама өңделмейді.

Түйіндік модель.

Дәстүрлі консенсус алгоритмінде түйіндер негізінен лидер-түйіндерге және консенсус түйіндеріне бөлінеді. Жаңа алгоритмде монитор концепциясы енгізілген. Түйіндердің әрқайсысының толық сипаттамасы төменде 2 кестеде берілген.

Кесте 2 - Түйіндердің әрқайсысының толық сипаттамасы

№	Түйін атаулары	Міндеті:	Артықшылықтары
1	Жалпы түйіндер (Full Nodes)	- Бүкіл блокчейн тарихын (ledger) толық сақтайды. - Барлық транзакцияларды тексеріп, оларды желіге таратады. - Желідегі басқа түйіндерге қажетті деректерді ұсынады.	Жоғары сенімділік: кез келген уақытта блокчейннің толық көшірмесін ұсынуға қабілетті.
2	Прокси-түйіндер (Proxy Nodes)	- Сегмент ішінде транзакцияларды өңдейді. - Клиенттердің сұрауларын қабылдап, оларды локалды консенсус арқылы өңдейді. - Алынған блоктарды Глобал прокси-түйіндерге жібереді	Масштабталуды арттырады, себебі барлық түйіндер бірден барлық транзакцияларды өңдемейді.
3	Глобал прокси-түйіндер (Global Proxy Nodes)	- Барлық сегменттерден ақпарат жинайды. - Әр сегменттен алынған блоктарды біріктіріп, бірыңғай блок құрайды. - Құрылған жаңа глобал блокты басқа прокси-түйіндерге таратады.	Желі тұрақтылығын сақтайды – әрбір сегмент жеке жұмыс істегенімен, глобалды блок арқылы барлық сегменттер бірдей синхрондалады.
4	Басқарушы түйіндер (Super Nodes)	- Түйіндердің мінез-құлқын бақылайды. - Аномалияларды анықтап, зиянкес түйіндерді блоктайды	Басқарушы түйіндер зиянкес түйіндерді анықтап, жүйенің тұрақтылығын

Консенсус түйіндері

Жүйеде консенсусқа қатысатын репликалар консенсус түйіндері деп аталады. Консенсус түйіндері – бұл блокчейн жүйесінде транзакцияларды тексеруге, блоктарды растауға және консенсусқа қол жеткізуге жауапты арнайы желі қатысушылары. Бұл түйіндер желідегі сенімділік пен қауіпсіздікті қамтамасыз етеді, себебі олар ереже бойынша жұмыс істейді және жүйенің шынайылығын сақтайды.

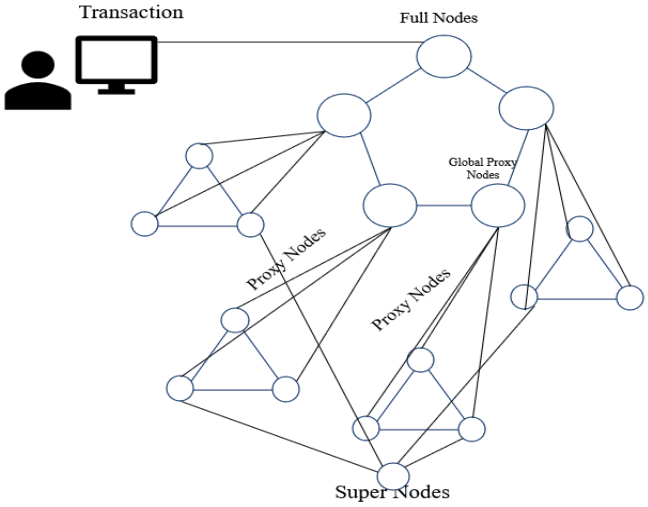
Біздің алгоритм сегментацияланған консенсусқа негізделгендіктен, онда түйіндер әртүрлі рөлдерге бөлінеді. Бұл архитектура блокчейннің масштабталуын, қауіпсіздігін және тиімділігін арттыруға мүмкіндік береді. Жаңа консенсус алгоритмі төрт деңгейлі түйіндер жүйесін қолданады, бұл масштабталу мен қауіпсіздікті жақсартады (Абдулжалилов 2023)

Сонымен:

- Жалпы түйіндер бүкіл блокчейн тарихын сақтайды.
- Прокси-түйіндер локалды консенсус жүргізіп, жүктемені азайтады.
- Глобал прокси-түйіндер барлық сегменттерден блоктарды біріктіреді.
- Басқарушы түйіндер зиянкес түйіндерді анықтап, жүйенің тұрақтылығын қамтамасыз етеді.

$N \geq 3f + 1$ формула бойынша, егер жүйеде N түйін болса, оның f түйіні Византиялық шабуылдаушы болуы мүмкін. Қауіпсіз консенсус үшін түйіндер саны $N \geq 3f + 1$ болу керек.

Консенсус түйіндері транзакцияларды тексеріп, желінің қауіпсіз жұмыс істеуін қамтамасыз етеді.



Сурет 2 - Түйіндерді сегменттеу құрылымы

Лидер түйін 2 - суретте Full Nodes бұл блокчейн немесе консенсус алгоритміндегі негізгі басқарушы түйін, яғни желі ішіндегі басқа түйіндердің әрекеттерін үйлестіріп, транзакцияларды ұсынатын және блоктарды жасайтын басты қатысушы.

Лидер жіберген і-нөмірлі түйін N_i келесідей анықталады: Барлық консенсусқа қатысатын түйіндер жиынтығы G символымен белгіленеді. $N_i(i=[1,n], N_i) \in G$ Түйін G ішіндегі басқа түйіндермен консенсус механизмін орнатады.

$$G = (N_1, N_2, \dots, N_i, \dots, N_n) \quad (1)$$

$$N_i = (G_i, st_i, h_i, v_i, l_i, S_i, C_i) \quad (2)$$

1 теңдеуде:

Gi - түйіннің келісілген идентификаторы және IP-мекенжайлар тізімі сақталған (түйін өзі сақтамайды).

st_i - түйіннің күйі, яғни ол лидер, $st_i \in$ орынбасар немесе жай консенсус түйіні екенін білдіреді.

h_i - блок биіктігі – түйін соңғы күйіне жеткен кезде.

v_i - көру нөмірі – консенсус циклы аяқталған кезде және лидер жұбы өзгергенде жаңартылады.

l_i -лидер индексі – мәні консенсус циклы аяқталғаннан кейін немесе орынбасар жаңа лидерлікке талас бастағанда ғана өзгеруі мүмкін.

S_i - гүйіннің орналасқан сегменттерінің тізімі – түйін тек өз сегментіндегі транзакцияларды өңдейді.

G_i - гарантия мәні – консенсус түйінінің басқа түйіндерге берген кепілдігі. Монитор түйіні гарантия сұранысын жіберген сайын бұл мән жаңартылып отырады.

Лидер түйін деген ұғым бар бірақ ол классикалық PBFT алгоритмінде бір лидер таңдалады. Лидер түйін деген жаңа блоктарды ұсынады, транзакцияларды реттейді, консенсусқа бағыт береді. Егер лидер бұзылса немесе дұрыс жұмыс істемесе, желі жаңа лидер сайлайды.

Дегенмен жаңа сегменттелген консенсус механизмінде бір орталықтандырылған лидер болмайды, бірақ прокси-түйіндер лидердің қызметін атқарады. Жергілікті (локалды) лидерлер – әрбір сегмент ішінде прокси-түйіндер транзакцияларды жинап, өңдейді. Глобалды лидерлер – глобал прокси-түйіндер барлық сегменттердің блоктарын біріктіреді. Бұл жүйе бір лидерге тәуелділікті азайтады, масштабтауды жақсартады және қауіпсіздікті күшейтеді. Лидердің болмауы қандай артықшылығы шабуылға төзімділік – дәстүрлі PBFT-те лидерге шабуыл жасалса, консенсус процесі баяулайды. Ұсынып отырған алгоритмде әр сегмент өз ішінде жұмыс істейді, сондықтан бүкіл жүйе бұзылмайды.

Бір лидердің орнына бірнеше прокси-түйіндер параллель жұмыс істейді, бұл TPS-ті яғни жылдамдықты арттырады. Масштабталу қосымша түйіндерді оңай қосуға болады, себебі әрқайсысы өз сегментінде жұмыс істейді (Дипа et al, 2016).

Блокчейндегі қолданыстағы PBFT консенсус алгоримдері N–N көп таралымдарын пайдаланады, бұл деректердің сәйкестігін қамтамасыз ету үшін жасалады. Алайда бұл әдіс блокчейн консенсус алгоритмдерінің өзара әрекеттесуінің күрделілігін арттырады және, көрініс өзгерісі орын алса PBFT $O(N^2)$ үшін $O(N^3)$ дейін жетуі мүмкін (Мерсер 2018). Салыстырмалы түрде Raft сияқты таратылған жүйенің консенсус алгоритмі байланыс күрделілігі O(N) болғанына қарамастан, сенімсіз ортада тиімді жұмыс істемейді. Оның лидері өте жоғары талаптарға сәйкес келуі керек, себебі ол бір уақытта көптеген түйіндерге хабар таратады. Егер лидер жұмысын тоқтатса немесе орын ауыстыруы қажет болса, бұл консенсусқа жету жылдамдығын төмендетеді, осылайша блокчейн жүйесінің орташа тиімділігіне әсер етеді.

Нәтижелер мен талқылаулар. Бұл мәселелерді шешу үшін, яғни блокчейн консенсус деңгейінің қауіпсіздік пен тиімділігінің жеткіліксіздігін жою үшін, келесі шешімдер ұсынылады:

1.Түйіндерге кепілдік беру механизмін енгізу – бұл түйіндер арасындағы сенімді қарым-қатынасты орнатуға мүмкіндік береді.

2.Сенімді түйін таңдау стратегиясын әзірлеу – бұл түйіндерді олардың өнімділігі мен мінез-құлқына негізделген бағалау моделін жасауға мүмкіндік береді.

3.Қосарлы көшбасшылық (екі лидер) бақылау механизмін енгізу – бұл таратылған транзакцияларды басқару үшін тиімді жұмыс істейді.

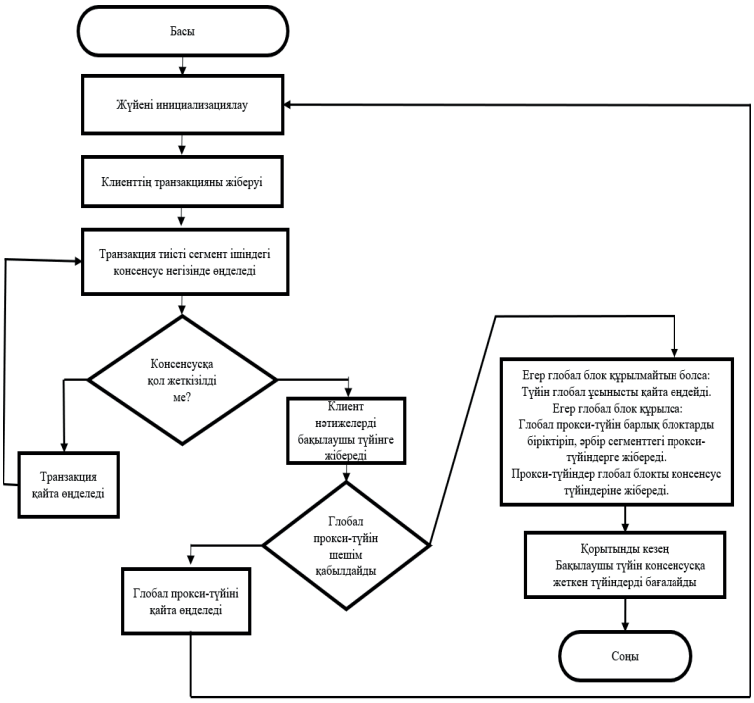
4.Консенсус бөліну моделін енгізу – лидерді сенімді таңдау стратегиясына сүйене отырып таңдау және механизм кепілдігі арқылы сегментацияны жүзеге асыру.

Осы шешімдерден қауіпсіз және масштабталатын консенсус алгоритмін әзірленеді – O(N) күрделілігімен жұмыс істейтін, бір уақытта консенсусқа қолдау көрсететін, сондай-ақ зиянды түйіндерді анықтап, алып тастайтын жүйе болып шығады.

Қазіргі сенім модельдері негізінен тікелей және жанама сенім модельдеріне бөлінеді:

Тікелей сенім моделі – түйіннің зиянды екенін тек оның мінез-құлқына сүйене отырып анықтайды. Бірақ бұл тәсіл әлсіз, өйткені сенімсіз модельдерді стратегия арқылы айналып өтуге мүмкіндік береді.

Жаңа PBFT негізінде құрылған алгоритмінің жүйелік орындалу процесі 3-суретте көрсетілген.



Сурет 3 - PBFT негізінде құрылған жаңа алгоритмнің жүйелік орындалу процесі

Алгоритмде түйіндерді сегментациялау бірнеше маңызды кезеңдерде жүзеге асады, бұл транзакцияларды параллель өңдеуді және жүктемені тиімді бөлуді қамтамасыз етеді.

Seg-PBFT Консенсус Алгоритмінің 9 Кезеңі (сегменттелген PBFT)

1-кезең: Сұраныс жіберу кезеңі (Request Phase)

Клиент өзінің сегментіндегі локалды прокси-түйінге сұраныс жібереді.

Бұл сұраныс ішкі сегмент ішінде талқыланып, консенсусқа келу үшін тіркеледі.

Клиент → Прокси

$$R_i = Request(T_x, C_i) \tag{3}$$

мұндағы T_x — транзакция, C_i — клиент, R_i — сұраныс.

2-кезең: Алдын ала дайындау кезеңі (Pre-Prepare Phase)

Прокси-түйін жаңа блок құрастырады.

Ол блокты сол сегменттегі басқа түйіндерге таратады.

Прокси → Сегменттегі түйіндер

$$B_j = CreateBlock(R_i) \tag{4}$$

және оны сегменттегі түйіндерге таратады:

$$\forall N_k \in S_j, \quad Send(B_j, N_k) \tag{5}$$

3-кезең: Дайындық – 1 (Prepare1 Phase)

Сегменттегі түйіндер бұл блокты тексереді.

Тексеруден кейін олар BLS мультиподпись (біріккен қолтаңба) жасап, оны прокси-түйінге қайтарады.

Түйіндер → Прокси

Әр түйін тексереді және қол қояды:

$$\sigma_k = Sign_{sk_k}(B_j)(\_k, P\_j) \tag{6}$$

4-кезең: Дайындық – 2 (Prepare2 Phase)

Прокси-түйін барлық қолтаңбаларды жинайды. 2f+1 түйіннен қол қойылғанда, ол оларды бір мультиподпиське біріктіріп, бүкіл сегментке таратады.

Прокси → Сегмент

Прокси 2f+1 қол жинап мультиподпись жасайды:

$$\Sigma_{prep} = \text{Aggregate}(\{\sigma_1, \sigma_2, \ldots, \sigma_{2f+1}\})(\_, S\_j) \tag{7}$$

5-кезең: Коммит – 1 (Commit1 Phase)

Түйіндер келген мультиподписьті тексереді. Егер қол қоюшылар саны ≥ 2f+1 болса — олар блокты тексереді және өз қолтаңбаларын береді.

Прокси → Сегмент

Әр түйін мультиподписьті тексереді:

$Verify(\Sigma_{prep})$

Содан кейін қол қояды:

$$\gamma_k = Sign_{sk_k}(B_j) \quad (8)$$

6-кезең: Коммит – 2 (Commit2 Phase)

Прокси-түйін тағы да 2f+1 қолтаңбаны жинап, бір BLS мультиподпиське біріктіреді. Бұл блокты барлық сегмент түйіндеріне жіберіп, соңғы растау үшін таратады.

Түйіндер → Клиент

Әр түйін клиентке жауап жібереді:

$$\Sigma_{commit} = Aggregate(\{\gamma_1, \ldots, \gamma_{2f+1}\}) \quad (9)$$

(_, S_j)

7-кезең: Жауап кезеңі (Response Phase)

Түйіндер клиентке жауап жібереді.

Клиент f+1 растаманы алса, консенсусқа жетті деген сөз.

Түйіндер → Клиент

Әр түйін клиентке жауап жібереді:

$Send(ACK_k, C_i)$

Клиент тексереді:

$$\#\{ACK\} \geq f + 1 \Rightarrow Consensus\ Achieved \quad (10)$$

8-кезең: Кері байланыс кезеңі (Feedback Phase)

Клиент барлық жауаптарды бас басқарушы түйінге жібереді.

Басқарушы түйін әр сегменттен алынған мәліметтерді тексеріп, сараптайды.

Клиент → Бас түйін

Клиент жауаптарды жібереді:

$$Send(\{ACK_k\}, L) \quad (11)$$

мұндағы L — бас басқарушы түйін.

9-кезең: Біріктіру және тарату кезеңі (Merge & Propagation Phase)

Сегменттік прокси-түйіндер локалды блоктарды жоғары деңгейдегі глобалды прокси-түйінге жібереді.

Прокси-сегменттер → Глобалды прокси

Глобал түйін бұл блоктарды біріктіріп, глобал блок жасап, жүйеге таратады.

Сегменттік блоктар:

$\{B_1, B_2, \ldots, B_m\}$

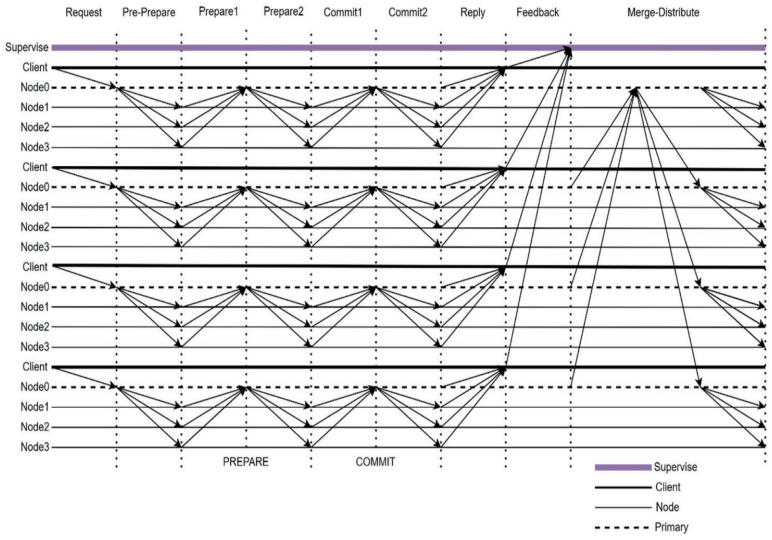
Глобалды блок құралады:

$$B_G = Merge(\{B_1, \ldots, B_m\}) \quad (12)$$

(B_G,)

Түйіндер сегментацияланады тікелей сұраныс кезеңінде – клиент әрдайым тек өз сегментімен әрекеттеседі. Консенсустың барлық алдын ала фазалары (Pre-Prepare, Prepare1, Prepare2, Commit1, Commit2) тек ішкі сегмент ішінде орындалады, глобалды түйіндермен өзара әрекеттесу болмайды. Тек соңғы кезеңде (Merge & Propagation) ғана локалды блоктар біріктіріліп, глобалды блок жасалады.

PBFT негізіндегі жаңа алгоритмі түйіндерді осылайша сегменттейді: консенсустың көп бөлігі локалды түрде орындалады, бұл желіге түсетін жүктемені азайтады. Тек соңғы кезеңде сегменттер өзара әрекеттесіп, бірыңғай глобалды блокты құрайды. Бұл тәсіл дәстүрлі PBFT алгоритмімен салыстырғанда масштабталуын, жылдамдығын және қауіпсіздігін жақсартады.



Сурет 4 - Алгоритмінің консенсус протоколымен өзара әрекеттесу үдерісі

4 - суретте көрсетілгендей консенсусқа жету процесі үш кезеңнен тұрады: pre−prepare, prepare және commit. Клиенттен сұраныс алғаннан кейін, негізгі түйін (яғни, Replica 0) pre−prepare хабарламасын басқа түйіндерге таратады. Prepare және commit кезеңдерінде әрбір реплика алынған хабарламалардың дұрыстығын тексеру үшін хабарламалар жібереді. Келесі кезеңге өту үшін қажетті минималды санды келісілген хабарламалар болуы керек.

PBFT негізіндегі жаңа консенсус механизмімен деректерді беру процесі басқа консенсус механизмдерінен айырмашылығы лидерлер әрбір резервтік көшірмеден транзакцияларды алған кезде консенсус терезесінің кезеңін динамикалық түрде реттейді. Лидер келесі кезеңнің уақытын ағымдағы кезеңде алынған транзакциялардың санына байланысты есептейді және оны

әрбір резервтік көшірмеге қайтарылған ақпаратпен бірге жібереді. Егер лидер бір уақытта көбірек транзакция алса, келесі кезеңнің уақыты қысқарады, сондықтан түйіннен жіберілген транзакцияларды жылдам өңдеуге болады. Ал керісінше, егер транзакциялар аз болса, келесі кезеңнің уақыты арттырылады, бұл желілік ресурстарды үнемдеуге мүмкіндік береді.

Төменде консенсус алгоритміндегі сұраныстарды өңдеудің негізгі кезеңдерінің бағдарламалық жүзеге асырылуы көрсетілген. Код Python тілінде жазылған және негізгі кезеңдерді қамтиды: сұраныс беру, блокты дайындау, қол қою және финализациялау.

```
def submit_request(self, client, data):
self.request_count += 1
self.requests[self.request_count] = {
«client»: client,
«data»: data,
«finalized»: False}
print(f»Request {self.request_count} submitted by {client}»)
return self.request_count

def prepare_block(self, request_id):
   if request_id not in self.requests:
raise ValueError(«Invalid request ID»)
print(f»Block prepared for request {request_id}»)

def sign_block(self, request_id, signer, signature):
if request_id not in self.signatures:
self.signatures[request_id] = []
self.signatures[request_id].append({«signer»: signer, «signature»: signature})

def commit_block(self, request_id):
if request_id not in self.signatures or len(self.signatures[request_id]) < 2:
raise ValueError(«Not enough signatures to commit»)
self.requests[request_id][«finalized»] = True
print(f»Request {request_id} committed successfully»)

def get_request(self, request_id):
   return self.requests.get(request_id, «Request not found»)
```

Ұсынылған модельдің тиімділігін бағалау

Бағалауды масштабталу параметрлері арқылы жүргіземіз

- Консенсус кідірісі (Latency) – транзакцияның расталуы үшін қажетті уақыт.

- Транзакция жылдамдығы (TPS) – блокчейн секундына қанша транзакцияны өңдей алады.

1.Консенсус кідірісі (Consensus Latency, мс)

Консенсус кідірісін келесі формула арқылы анықталады:

$$L_{\text{consensus}} = T_{\text{propose}} + T_{\text{network}} + T_{\text{verify}} + T_{\text{commit}} \quad (13)$$

Мұндағы:

$L_{consensus}$ - жалпы консенсус кідірісі (мс)

$T_{propose}$ - блок ұсынылу уақыты (лидер немесе прокси-түйін жаңа блокты ұсынады)

$T_{network}$ - желіде хабарламаларды тарату уақыты (latency)

T_{verify} - түйіндердің блоктағы транзакцияларды тексеру уақыты

T_{commit} - блоктың бекітілу уақыты (коммит фазасы)

Егер жүйе сегменттелетін болса, әрбір сегменттің кідірісі жеке есептеліп, жалпы жүйенің кідірісі ең баяу сегменттің кідірісіне тең:

$$L_{\text{total}} = \max(L_1, L_2, \dots, L_n) \quad (14)$$

мұнда L_i— і-ші сегменттің консенсус кідірісі.

Тестілеу: Әдетте желі топологиясын жобалау Cisco Packet Tracer немесе GNS3 көмегімен орындалады. Біз GNS3 қолданамыз ол қажетті сұлбаларды немесе шешімдерді модельдеуге, конфигурацияны нақты жабдықта қолданбас бұрын тексеруге болатын толыққанды зертханалық құрал.

Тестілеу барысында жүйеге 1000 транзакция жіберілді. Блоктың ұсынылған уақыты (Tpropose) және соңғы бекітілген блоктың уақыты (Tcommit) тіркелді.

Блок деңгейінде:

$$L_{\text{block}} = T_{\text{commit}} - T_{\text{propose}} \quad (15)$$

Орташа мәні:

$$L_{\text{avg}} = \frac{\sum L_{\text{block}}}{N} \quad (25)$$

мұндағы N — жалпы блок саны.

Бір блоктың ұсынылу уақыты 48 мс, желідегі кешігу 32 мс, тексеру уақыты 21 мс, ал бекіту уақыты 46 мс болды

$$L_{\text{consensus}} = 48 + 32 + 21 + 46 = 147\ mc \quad (16)$$

Бұл блокчейннің орташа консенсус кідірісі 147 мс екенін көрсетті.

PBFT және оның туындылары негізінде жасалған консенсус алгоритмдердің көрсеткіштерін әдебиеттік зерттеу жұмыстарынан алынып, PBFT негізіндегі жаңа консенсус алгоритммен салыстырмалы түрде қарастырылады. Бұл салыстыру жүйенің ақауға төзімділігі, масштабталуы, уақытша кідіріс және байланыс күрделілігі сияқты негізгі параметрлерге сүйенеді.

Кесте 3 - PBFT және оның туындылары негізінде жасалған консенсус алгоритмдерінің салыстырмалы сипаттамасы

Алгоритм	Ақауға төзімділік	Масштабталуы	Кідіріс	Байланыс күрделілігі
IBFT	$3f + 1$	Төмен	Төмен	$O(n^2)$
RBFT	$2f + 1$	Орташа	Төмен	$O(n^4)$
PoET	–	Жақсы	Орташа	$O(n^3)$
PBFT	$3f + 1$	Орташа	200–500 мс	$O(n^2)$ (шамамен)
PBFT негізіндегі жаңа алгоритм	$2f + 1$	Жақсы	80–147 мс	$O(n)$–$O(n^2)$ (оңтайландырылған)

Салыстырма үшін IBFT алгоритмі ақауға төзімділік жағынан PBFT-ке ұқсас, бірақ масштабталу мүмкіндігі шектеулі, сондықтан тек кішігірім желілер үшін тиімді. RBFT байланыс күрделілігін төмендетуге бағытталғанымен, оның есептеу ресурстарына қойылатын талаптары жоғары ($O(n^4)$), бұл үлкен желілерде қолдануға кедергі келтіреді. PoET алгоритмі рұқсат етілмеген (permissionless) жүйелерге бағытталған және масштабталу мүмкіндігі жоғары болғанымен, қауіпсіздігі сенімге негізделген.

PBFT алгоритмі орташа кідіріс уақыты мен күрделілігіне ие және көптеген консорциумдық блокчейндерде әлі де кеңінен қолданылады. Алайда, оның байланыс күрделілігі $O(n^2)$ деңгейінде болуы үлкен желілерде өнімділікті төмендетеді.

Ұсынылып отырған жаңа алгоритм осы мәселелерді шешуге бағытталған. Ол желіні сегменттерге бөлу арқылы көшбасшыны ауыстыру механизмін оңтайландырады. Бұл тәсіл кідірісті 80–147 миллисекунд аралығына дейін қысқартып, консенсус процесінің өнімділігін арттырады. Сонымен қатар, байланыс күрделілігі дәстүрлі PBFT-пен салыстырғанда төмен ($O(n)$–$O(n^2)$), бұл оны масштабталатын жүйелер үшін қолайлы етеді. Ақауға төзімділік те оңтайлы деңгейде сақталған — тек $2f + 1$ түйін жеткілікті, бұл жүйенің ресурстық тиімділігін арттырады.

Кесте 4 - PBFT және PBFT негізіндегі жаңа алгоритмдерінің салыстырмалы талдауы

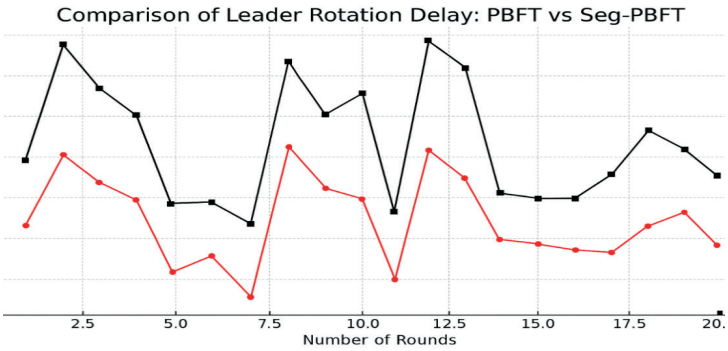
Параметр	PBFT	PBFT негізіндегі жаңа алгоритм	Айырмашылығы
Ақауға төзімділік	$3f + 1$	$2f + 1$	33% жеңілдік — азырақ түйінмен консенсусқа жетеді
Кідіріс	200–500 мс	80–147 мс	Орта есеппен 62–70% жылдамырақ

Масштабталуы	20–100 түйін	180+ түйін)	>100% жоғары — екі есе көп түйінді қолдай алады
Байланыс күрделілігі	$O(n^2)$	$O(n)$–$O(n^2)$ (оңтайландырылған)	Күрделілік төмендеген – тиімділік жақсарған

Жоғарыдағы салыстыру PBFT және оның жетілдірілген нұсқасы PBFT негізінде құрылған жаңа алгоритмнің арасындағы маңызды айырмашылықтарды көрсетеді. Бұл алгоритм көшбасшыны ауыстыру және түйіндер құрылымын сегменттеу арқылы бірнеше көрсеткіш бойынша айтарлықтай артықшылыққа ие:

- Ақауға төзімділікте $3f + 1$ орнына $2f + 1$ қолдану жүйенің қажетті түйін санын 33%-ға азайтып, ресурстық тиімділікті арттырды.
- Кідіріс уақыты бойынша орта есеппен 2.5–3 есе жылдам жұмыс істейді (500 мс орнына 147 мс).
- Масштабталуы бойынша PBFT негізіндегі жаңа алгоритм 180 және одан да көп түйінмен тиімді жұмыс істей алады, бұл PBFT-пен салыстырғанда екі есе көп.
- Байланыс күрделілігі $O(n^2)$-ден $O(n)$–$O(n^2)$-ге оңтайландырылып, желі трафигі мен жүктемесі азаяды, әсіресе үлкен желілерде.

PBFT және PBFT негізіндегі жаңа алгоритм алгоритмдері бойынша лидерді ауыстыруға кеткен уақыттың салыстырмалы графигі Сурет 5 ұсынылған.



Сурет 5 - PBFT пен PBFT негізінде құрылған жаңа алгоритмдерінің консенсус кідірісін салыстырмалы талдау графигі

Горизонталь ось – эксперименттік раундтардың саны (жалпы 20 топ), ал вертикаль ось – лидерді ауыстыруға кеткен уақыт (миллисекундпен, мс).

Қорытынды. Бұл зерттеуде консенсус алгоритмдерінің ішінде лидерді ауыстыру уақытына ерекше назар аударылды. PBFT және PBFT негізіндегі жаңа алгоритм алгоритмдері бойынша жүргізілген эксперименттік бағалау нәтижелері блокчейн жүйелерінің ақауға төзімділігі мен байланыс күрделілігіне қатысты маңызды мәліметтер береді.

Зерттеу барысында алгоритмдер Python тілінде симуляцияланып,

нәтижелер Matplotlib кітапханасы арқылы визуалданды. Бұл тәсіл желілік протоколдардың жұмысын нақты көрсетіп, оңтайландыру мүмкіндіктерін анықтауға мүмкіндік берді (Мельников et al, 2009). PBFT алгоритмінің негізінде сипатталған жаңа алгоритм бір үлгіге орналастырып, нақты салыстыру жүргіздік. Авторлар екі алгоритмді де 20 топта сынап көріп, уақытша кідірістерді есептеді, және эксперимент нәтижелері 5- суретте көрсетілген.

Эксперимент нәтижелері көрсеткендей жаңа алгоритм жүйесіндегі көшбасшыны басқару механизмі PBFT алгоритміне қарағанда орындау уақыты бойынша 62-70% тиімдірек. PBFT негізінде құрылған жаңа алгоритм негізгі түйінді көшбасшының тоқтап қалуынан кейін жылдамырақ ауыстыра алады және консенсусқа қол жеткізу процесіне әсерін азайтады. Осылайша бұл алгоритм шешімдердің эволюциясында жаңа қадам болып табылады. Ол масштабталу, жылдамдық және қауіпсіздік тұрғысынан теңгерімді қамтамасыз етіп, заманауи блокчейн жүйелерінің талаптарына жақсырақ жауап береді.

Әдебиеттер

Bonneau J., Miller A., Clark J., Narayanan A., Kroll J.A., Felten E.W. SoK. (2015) Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy. — P. 104–121. doi: 10.1109/SP.2015.14.

Buchaesi M., Кальзавара С., Фокарди Р. (2017) Формальные методы веб-безопасности. Журнал логических и алгебраических методов в программировании. — Т. 87. — С. 110–126.

Huynh T.T., Huynh T.D., Nguyen H., Tan H.A (2019) Survey on security and privacy issues of blockchain technology. Proc. 2019 IEEE Int. Conf. Syst. Sci. Eng. — P. 362–367.

Leng J., Zhou M., Zhao J.L., Huang Y., Bian Y. (2022) Blockchain security: A survey of techniques and research directions. IEEE Trans. Serv. Comput. — Vol. 15, No. 4. — P. 2490–2510.

Li X., Jiang P., Chen T., Luo X., Wen Q.A. (2020) Survey on the security of blockchain systems. Future Gener. Comput. Syst., Vol. 107. — P. 841–853.

Popadyuk A.Yu., Korovyakovsky E.K., Titova T.S. (2020) Environmental Aspects of Distributed Ledger Technology: A Case Study of the Proof-of-Work Consensus Algorithm. Proc. of the St. Petersburg State University of Railway Communications. — Т. 17. — №1. — P. 136–143.

Sompolinsky Y., Lewenberg Y., Zohar A. (2016) Inclusive Block Chain Protocols. International Conference on Financial Cryptography and Data Security. Springer, — P. 528–547. DOI: 10.1007/978-3-662-53357-4_26.

Somin S., Gordon G., Altshuler Y. (2018) Network analysis of ERC20 tokens trading on Ethereum blockchain. In: Unifying Themes in Complex Systems IX. Cham: Springer, — P. 439–450.

Абдулжалилов А.З. (2023) Методы и стратегии масштабируемости блокчейн-технологий: анализ, сравнение и перспективы, Вестник науки. — №11(68). — Т 4. — С. 625–634.

Баракова А.Ш., Усатова О.А. (2022) Веб-ресурстардың қауіпсіздігінің осалдықтары мен қауіптерін жіктеу және сипаттау Материалы VII международной научно-практической конференции «Информатика и прикладная математика». Алматы. — С. 364–368.

Вуколич М.В (2015) Поисках масштабируемой блокчейн-сети: доказательство выполнения работы против репликации BFT, Материалы Международного семинара по открытым проблемам сетевой безопасности. — С. 112–125.

Дипа Г., Тилагам П. С. (2016) Защита веб–приложений от уязвимостей, связанных с внедрением и логикой: подходы и проблемы информационные *и программные технологии.* — Т. 74. — С. 160–180.

Усатова О.А., Баракова А.Ш. (2022) Қазіргі заманғы веб-ресурстарды қорғау жүйелерін

талдау. ҚР ҰҒА Хабарлары. Физика және информатика сериясы, №1 (341). — Б. 88–95. *https://doi.org/10.32014/2022.2518-1726.120*

Мерсер Д. (2018) Создание надёжных и полнофункциональных веб-сайтов, блогов, форумов, порталов и сайтов-сообществ. — М.: Вильямс. — С. 272–274.

Мельников В.П., Клейменов С.А., Петраков А.М. (2009) Информационная безопасность и защита информации: учебник. — С. 184–186.

References

Bonneau J., Miller A., Clark J., Narayanan A., Kroll J.A., Felten E.W. SoK. (2015) Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy. — P. 104–121. doi: 10.1109/SP.2015.14. (in Eng)

Buchaezi M., Kalzavara S., Fokardi R. (2017) Formal'nye metody veb-bezopasnosti [Formal Methods of Web Security]. Journal of Logical and Algebraic Methods in Programming. — T. 87. — P. 110–126. (in Rus)

Huynh T.T., Huynh T.D., Nguyen H., Tan H.A (2019). survey on security and privacy issues of blockchain technology. Proc. 2019 IEEE Int. Conf. Syst. Sci. Eng. — P. 362–367. (in Eng)

Leng J., Zhou M., Zhao J.L., Huang Y., Bian Y. (2022). Blockchain security: A survey of techniques and research directions. IEEE Trans. Serv. Comput. — Vol. 15. — No. 4. — P. 2490–2510. (in Eng)

Li X., Jiang P., Chen T., Luo X., Wen Q.A(2020) Survey on the security of blockchain systems. Future Gener. Comput. Syst., Vol. 107. — P. 841–853. (in Eng)

Popadyuk A.Yu., Korovyakovsky E.K., Titova T.S. (2020) Environmental Aspects of Distributed Ledger Technology: A Case Study of the Proof-of-Work Consensus Algorithm. Proc. of the St. Petersburg State University of Railway Communications. — T. 17. — №1. — P. 136–143. (in Eng)

Sompolinsky Y., Lewenberg Y., Zohar A. (2016) Inclusive Block Chain Protocols. International Conference on Financial Cryptography and Data Security. Springer. — P. 528–547. DOI: 10.1007/978-3-662-53357-4_26. (in Eng)

Somin S., Gordon G., Altshuler Y. (2018) Network analysis of ERC20 tokens trading on Ethereum blockchain. In: Unifying Themes in Complex Systems IX. Cham: Springer. — P. 439–450. (in Eng)

Abdulzhalilov A.Z. (2023) Metody i strategii masshtabiruemosti blokchein-tekhnologii: analiz, sravnenie i perspektivy [Methods and Strategies for Blockchain Scalability: Analysis, Comparison, and Prospects]. Vestnik nauki. — №11(68). — T 4. — P. 625–634. (in Rus)

Barakova A.Sh., Usatova O.A. (2022) Veb-resurstardyn kaúipsizdiginiń osaldyqtary men kaúpterin zhikteu jáne sipattau [Classification and Description of Web Resource Security Vulnerabilities and Threats]. Materialy VII mezhdunarodnoi nauchno-prakticheskoi konferentsii «Informatika i prikladnaia matematika». Almaty. — P. 364–368. (in Rus)

Vukolich M.V. (2015) Poiskakh masshtabiruemoi blokchein-seti: dokazatel'stvo vypolneniia raboty protiv replikatsii BFT [In Search of a Scalable Blockchain Network: Proof-of-Work versus BFT Replication]. Materialy Mezhdunarodnogo seminara po otkrytym problemam setevoi bezopasnosti. — P. 112–125. (in Rus)

Dipa G., Tilagam P.S. (2016) Zashchita veb-prilozhenii ot uiazvimostei, sviazannykh s vnedreniem i logikoi: podkhody i problemy. Informatsionnye i programmnye tekhnologii [Protection of Web Applications from Injection and Logic-Related Vulnerabilities: Approaches and Challenges]. — T. 74. — P.160–180. (in Rus)

Usatova O.A., Barakova A.Sh. (2022) Qazirgi zamangy veb-resurstardy qorgau zhüielerin taldau [Analysis of Modern Web Resource Protection Systems]. Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. Series of Physics and Informatics, №1 (341). — P. 88–95. https://doi.org/10.32014/2022.2518-1726.120 (in Kaz)

Mercer D. (2018) Sozdanie nadezhnykh i polnofunktsional'nykh veb-saitov, blogov, forumov, portalov i saitov–soobshchestv [Creating Reliable and Fully Functional Websites, Blogs, Forums, Portals, and Community Sites]. — M.: Vil'iams, — P. 272–274. (in Rus)

Melnikov V.P., Kleimenov S.A., Petrakov A.M. (2009) Informatsionnaia bezopasnost' i zashchita informatsii [Information Security and Information Protection]. Textbook. — P. 184–186. (in Rus)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Ответственный редактор *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Т. Апендиев*
Верстка на компьютере: *Г.Д. Жадырановой*

Подписано в печать 22.12.2025.
Формат 60x881/8. Бумага офсетная.
Печать –ризограф. 20,0 п.л. Заказ 4.

«Central Asian Academic Research Center» LLP
Алматы, Қонаев к-сі, 142