информационные системы

Компьютерные инструменты в образовании, 2023
№ 3: 28–34
УДК: 004.657
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-28-34

СИСТЕМНАЯ ИНТЕГРАЦИЯ И ОПТИМИЗАЦИЯ БЕЗОПАСНОСТИ В МНОГОУРОВНЕВОЙ ВИРТУАЛЬНОЙ СЕТИ

Щеголева Н. Л.[1], доктор техн. наук, доцент, n.shchegoleva@spbu.ru,
orcid.org/0000-0003-1087-2833
Киямов Ж. У.[1], преподаватель-исследователь, ✉ z.kiyamov@spbu.ru,
orcid.org/0000-0002-8623-1090

[1]Санкт-Петербургский государственный университет,
Университетский пр., д. 35, Старый Петергоф, 198504, Санкт-Петербург, Россия

Аннотация

В современных распределенных системах, особенно в области блокчейн и облачных вычислений, обеспечение надежного и эффективного консенсуса является критически важной задачей. В данной работе рассматривается комбинированный подход обеспечения консенсуса, основанный на сочетании протоколов P-BFT и RAFT с точки зрения возможности повышения надежности, производительности и безопасности его использования в распределенных реестрах и облачных системах. Изложены принципы работы и характеристики каждого протокола, а также их совместное использование для достижения согласия в распределенной среде. Выполнен анализ преимуществ и перспектив использования комбинации протоколов P-BFT и RAFT, особенностей поддержки различных моделей доверия, а также интеграции механизмов защиты данных для обеспечения безопасности и конфиденциальности. Полученные результаты позволяют утверждать, что применение комбинации протоколов P-BFT и RAFT в распределенных реестрах и облачных системах обеспечивает их высокую производительность и надежность, что определяет перспективность применения в различных областях, где требуется надежный и безопасный консенсус для обеспечения эффективной работы распределенных систем.

Ключевые слова: *распределенный реестр, блокчейн, P-BFT, RAFT.*

Цитирование: Щеголева Н. Л., Киямов Ж. У. Системная интеграция и оптимизация безопасности в многоуровневой виртуальной сети // Компьютерные инструменты в образовании. 2023. № 3. С. 28-34. doi: 10.32603/2071-2340-2023-3-28-34

1. ВВЕДЕНИЕ

На сегодняшний день для распределенных систем, особенно в области блокчейн и облачных вычислений, предложено большое количество алгоритмов консенсуса, каждый из которых позволяет решить определенный круг задач и имеет свои преимущества и недостатки. Однако, несмотря на большое количество исследований в данной области, до настоящего времени не предложено универсального алгоритма консенсуса, который подходил бы для всех систем вне зависимости от области применения. Поэтому наибо-

лее перспективным направлением исследований является комбинирование нескольких консенсусов, что обусловлено следующими причинами:

1. **Производительность.** Некоторые протоколы консенсуса, такие как PBFT (Practical Byzantine Fault Tolerance), обеспечивают высокую скорость и отказоустойчивость, но при этом требуют большого количества сообщений и обменов между узлами, что может привести к снижению производительности системы [1, 2].
2. **Гибкость.** Различные приложения и сценарии использования требуют разных свойств консенсуса, например таких, как линейная упорядоченность транзакций, низкая задержка подтверждения или гарантии безопасности. Одиночный протокол консенсуса может не обеспечить все необходимые свойства.
3. **Устойчивость к атакам.** Ряд протоколов консенсуса уязвим к определенным типам атак, таким как Sybil-атаки или атаки на узлы, то есть они не могут обеспечить надежную защиту [3, 4].
4. **Масштабируемость.** Некоторые протоколы консенсуса могут столкнуться с проблемами масштабируемости при увеличении числа участников, объема данных или при увеличении размера сети.
5. **Поддержка разных моделей доверия.** Разные приложения могут требовать разных моделей доверия, например доверие на основе репутации или доверие на основе веса узлов.

Комбинированный подход позволяет объединить преимущества различных протоколов консенсуса, преодолевая их ограничения и создавая более гибкую производительную и безопасную систему распределенного реестра.

2. ПРИМЕНЕНИЕ КОМБИНИРОВАННОГО ПОДХОДА В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Потребность в комбинированном подходе для улучшения консенсуса в распределенных реестрах возникает из-за необходимости решения описанных выше проблем и ограничений, связанных с традиционными протоколами консенсуса. При этом применение комбинированного подхода позволит:

— использовать преимущества нескольких протоколов, чтобы достичь более эффективного баланса между производительностью и безопасностью [5, 6];
— комбинировать несколько протоколов с разными свойствами для достижения оптимальных результатов;
— использовать несколько протоколов, которые совместно смогут устойчиво справляться с различными типами атак, повышая общую безопасность системы [7];
— предложить решения для повышения масштабируемости и обеспечения эффективной работы системы даже при увеличении размера сети или объема данных;
— комбинировать несколько протоколов, поддерживающих разные модели доверия, для адаптации к конкретным требованиям приложения.

Анализ существующих алгоритмов консенсуса показал, что наиболее перспективными для объединения в одной системе являются P-BFT и RAFT. Рассмотрим их характеристики подробнее.

Консенсус P-BFT был разработан для обеспечения высокой производительности и отказоустойчивости в системах с Byzantine-отказами. Высокая производительность достигается за счет оптимизации коммуникаций между узлами и использования репликации состояния. Небольшое время подтверждения транзакций в P-BFT обеспечивается благодаря частичной предварительной сортировке и линейной сложности для операций чте-

ния / записи. Поэтому данный консенсус обладает хорошей масштабируемостью, что позволяет эффективно работать с увеличением числа участников и объема данных [8].

P-BFT базируется на модели доверия, основанной на сети доверенных узлов [9]. Он предполагает, что большинство узлов в системе являются честными и не будут совершать вредоносных действий. Это позволяет достичь безопасности и отказоустойчивости системы.

Например, если приложение требует доверия на основе репутации, можно использовать P-BFT для обработки транзакций. В то же время, несмотря на высокую скорость и отказоустойчивость, P-BFT требует большого количества сообщений и обменов между узлами, что может снизить производительность системы. Тем не менее, данный консенсус может быть использован для обеспечения отказоустойчивости и поддержания консистентности данных.

Консенсус RAFT основывается на модели доверия лидеру — предполагается, что выбранный лидер для координации операций в распределенной системе будет действовать в интересах системы и корректно выполнять операции. RAFT обеспечивает безопасность и надежность путем репликации журнала операций и голосования при выборе лидера [10], обеспечивая минимальное время выбора нового лидера и быстрое восстановление после сбоев. Протокол RAFT имеет более простую архитектуру и меньшую нагрузку на сеть. Это способствует повышению производительности системы и хорошей масштабируемости, что позволяет эффективно работать с увеличением числа участников и объема данных, а также обеспечивать быстрое восстановление системы после сбоев.

При использовании комбинированного подхода можно воспользоваться преимуществами PBFT в отношении отказоустойчивости и скорости, а также внедрить протокол RAFT для улучшения производительности (рис. 1).

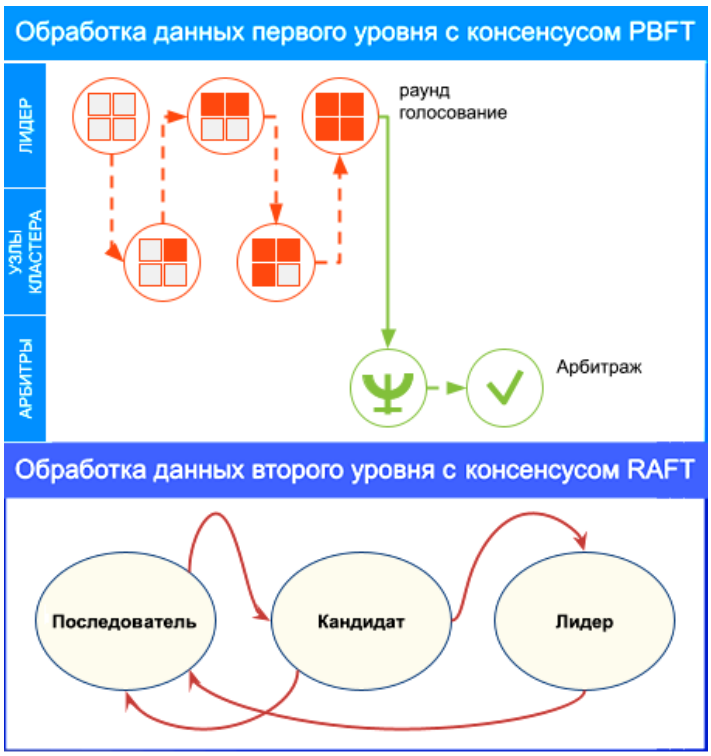

Рис. 1. Верхний и нижний уровень обработки данных

Путем комбинирования этих протоколов можно достичь оптимального баланса между производительностью и безопасностью в распределенном реестре. PBFT будет использоваться для обеспечения отказоустойчивости и поддержания консистентности данных, а RAFT будет использоваться для улучшения производительности и снижения нагрузки на сеть. Таким образом, комбинированный подход позволяет оптимизировать производительность системы и обеспечить высокий уровень безопасности [11].

Комбинированный подход обеспечивает гибкость в выборе и настройке протоколов консенсуса в соответствии с требованиями приложений. Он позволяет использовать наилучшие свойства каждого протокола, чтобы достичь оптимальной производительности, безопасности и других необходимых свойств, обеспечивая таким образом гибкость и адаптивность системы к различным сценариям и требованиям, повышая ее эффективность и функциональность.

Данный подход также может предложить механизмы горизонтального масштабирования, когда новые участники могут быть легко добавлены в систему без значительного влияния на ее производительность. Это может быть осуществлено, например, путем разделения сети на подгруппы или уровни, где каждая подгруппа может использовать свой протокол консенсуса, а основной протокол используется для достижения консенсуса между подгруппами [12, 13].

3. ПРЕИМУЩЕСТВА И ПЕРСПЕКТИВЫ КОМБИНИРОВАННОГО ПОДХОДА P-BFT И RAFT В РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ

Предлагаемый подход, объединяющий протоколы консенсуса P-BFT и RAFT, имеет следующие преимущества для распределенных реестров:

1. **Высокая производительность.** P-BFT и RAFT оба известны своей способностью обеспечивать высокую производительность системы. Комбинированный подход позволяет использовать преимущества обоих протоколов, такие как быстрое время подтверждения транзакций и высокая пропускная способность, что способствует более эффективной работе распределенного реестра.
2. **Безопасность и устойчивость.** P-BFT — протокол, обеспечивающий устойчивость к различным типам атак, включая Byzantine-атаки, где узлы могут вести себя вредоносно. RAFT предлагает лидерский подход к консенсусу, что делает систему более устойчивой к сбоям и отказам узлов. Комбинированный подход обеспечивает более надежный и безопасный консенсус, повышая общую устойчивость системы [14].
3. **Гибкость и адаптивность.** Комбинированный подход позволяет легко адаптироваться к различным требованиям и сценариям. Комбинирование различных протоколов консенсуса позволяет выбирать наиболее подходящие методы для определенных типов данных и ситуаций, что дает возможность наилучшим образом настроить систему в соответствии с требованиям конкретного приложения.
4. **Масштабируемость.** P-BFT и RAFT оба обладают хорошей масштабируемостью, что позволяет эффективно работать с увеличением числа участников и объема данных. Комбинированный подход на основе преимуществ обоих протоколов предлагает решения для повышения масштабируемости системы, обеспечивая эффективную работу при увеличении размера сети или объема данных [15].
5. **Поддержка разных моделей доверия.** P-BFT и RAFT оба поддерживают различные модели доверия. Комбинирование нескольких протоколов, поддерживающих разные модели доверия, делает систему более гибкой и способной адаптироваться к требованиям разных приложений.

В целом, реализация комбинированного подхода (P-BFT и RAFT) в распределенных реестрах обеспечивает высокую производительность, безопасность, гибкость, масштабируемость и поддержку разных моделей доверия. Этот подход является чрезвычайно перспективным для применения в различных сферах, где требуется надежный и эффективный консенсус в распределенных системах.

4. ЗАКЛЮЧЕНИЕ

Предложенный подход, использующий комбинацию P-BFT и RAFT, представляет собой мощный инструмент для обработки и анализа больших данных в распределенных сетях. Этот подход объединяет преимущества обоих алгоритмов, обеспечивая высокую производительность, безопасность и отказоустойчивость системы.

Метод P-BFT на верхнем уровне обработки транзакций обеспечивает быстрое достижение консенсуса между узлами и эффективную обработку больших объемов транзакций. При этом алгоритм RAFT на нижнем уровне обработки транзакций обеспечивает стабильность и надежность системы, позволяя быстро выбрать нового лидера и обрабатывать данные с минимальными задержками.

Комбинированный подход также обладает устойчивостью к сбоям и возможностью параллельной обработки данных, что позволяет системе эффективно работать даже при возникновении отказов в работе узлов или при обработке больших объемов данных.

Важным преимуществом комбинированного подхода является его гибкость и масштабируемость. Система может быть легко расширена путем добавления новых узлов, что позволяет удовлетворить растущие потребности в анализе больших данных.

В целом, комбинированный подход P-BFT и RAFT представляет собой перспективное решение для анализа больших данных в распределенных сетях, которое обеспечивает высокую производительность, безопасность, отказоустойчивость и эффективную работу в современной цифровой среде.

Список литературы

1. *Bogdanov A. et al.* A Multilayer Approach to the Security of Blockchain Networks of the Future // International Conference on Computational Science and Its Applications. Cham: Springer International Publishing, 2022. P. 205–216.
2. *Buchman E.* Tendermint: Byzantine fault tolerance in the age of blockchains. University of Guelph, 2016.
3. *Lin S. H., Liao M. H.* Towards publishing social network data with graph anonymization // Journal of Intelligent & Fuzzy Systems. 2016. Vol. 30, №. 1. P. 333–345.
4. *Zhu C. et al.* A Survey on the Integration of Blockchains and Databases // Data Science and Engineering. 2023. Vol. 8, № 2. P. 196–219.
5. *Liu K., Terzi E.* Towards identity anonymization on graphs // Proceedings of the 2008 ACM SIGMOD international conference on Management of data. 2008. P. 93–106.
6. *Zhang P., Zhou M.* Security and trust in blockchains: Architecture, key technologies, and open issues // IEEE Transactions on Computational Social Systems. 2020. Vol. 7, №. 3. P. 790–801.
7. *Vukolić M.* The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication // Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers. Springer International Publishing, 2016. P. 112–125.
8. *Ferguson N., Schneier B., Kohno T.* Cryptography engineering: design principles and practical applications. John Wiley & Sons, 2011.
9. *Lamport L., Shostak R., Pease M.* The Byzantine Generals Problem–ACM Transactions of Programming Languages and Systems // The Byzantine Generals Problem ACM Transactions on Programming Lanuages and Systems. 1982. Vol. 4, №. 3. P. 382–401.

10. *Castro M. et al.* Practical byzantine fault tolerance // OsDI. 1999. Vol. 99, №. 1999. P. 173–186.
11. *Pass R., Shi E.* Hybrid consensus: Efficient consensus in the permissionless model // Cryptology ePrint Archive. 2016. URL: https://eprint.iacr.org/2016/917 (date: ???).
12. *Bogdanov A. et al.* Testing and Comparative Analysis of the F-BFT-based DLT Solution // Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part IV 21. Springer International Publishing, 2021. P. 31–41.
13. *Zhou J. et al.* A Hybrid Consensus Algorithm for Blockchain // 2019 IEEE 5th International Conference on Computer and Communications (ICCC). IEEE, 2019.
14. *Zhang Y. et al.* A survey on software defined networking with multiple controllers // Journal of Network and Computer Applications. 2018. Vol. 103. P. 101–118.
15. *Khan M. A.* A survey of security issues for cloud computing // Journal of network and computer applications. 2016. Vol. 71. P. 11–29.

Поступила в редакцию 22.06.2023, окончательный вариант — 17.08.2023.

Щеголева Надежда Львовна, доктор технических наук, профессор кафедры фундаментальной информатики и распределенных систем СПбГУ, n.shchegoleva@spbu.ru

Киямов Жасур Уткирович, ассистент кафедры компьютерного моделирования и многопроцессорных систем СПбГУ, ✉ z.kiyamov@spbu.ru

Computer tools in education, 2023
№ 3: 28–34
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-28-34

System Integration and Optimization of Security in a Multilayer Virtual Network

Shchegoleva N. L.[1], Doctor sc., Associate Professor, n.shchegoleva@spbu.ru, orcid.org/0000-0003-1087-2833
Kiyamov J. U.[1], Teacher-researcher, ✉ z.kiyamov@spbu.ru, orcid.org/0000-0002-8623-1090
[1]Saint Petersburg State University, 35 Universitetskiy pr., Stary Peterhof, 198504, Saint Petersburg, Russia

Abstract

In modern distributed systems, especially in the field of blockchain and cloud computing, ensuring reliable and efficient consensus is a critical task. This paper discusses a combined consensus approach based on a combination of P-BFT and RAFT protocols. The purpose of this study is to explore the possibilities of a combined P-BFT and RAFT consensus approach to improve reliability, performance and security in distributed registries and cloud systems. The principles of operation and characteristics of each protocol are explored, as well as their joint use to achieve agreement in a distributed environment. In the course of the work, the advantages and prospects of the combined P-BFT and RAFT approach are analyzed, support for various trust models is considered, as well as the integration of data protection mechanisms to ensure security and privacy. The results of the study suggest that the combined P-BFT and RAFT consensus approach demonstrates high performance and reliability in distributed registries and cloud systems. The proposed approach has

prospects for application in various areas where a reliable and secure consensus is required to ensure the efficient operation of distributed systems.

Keywords: *distributed ledger, blockchain, P-BFT, RAFT.*

Citation: N. L. Shchegoleva and J. U. Kiyamov, "System Integration and Optimization of Security in a Multilayer Virtual Network," Computer tools in education, no. 3, pp. 28-34, 2023 (in Russian); doi: 10.32603/2071-2340-2023-3-28-34

References

1. A. Bogdanov et al., "A Multilayer Approach to the Security of Blockchain Networks of the Future," in *Proc. Int. Conf. on Computational Science and Its Applications*, Cham: Springer International Publishing, pp. 205–216, 2022; doi:10.1007/978-3-031-10536-4_14.
2. E. Buchman, *Tendermint: Byzantine fault tolerance in the age of blockchains*, Guelph, Ontario, Canada: University of Guelph, 2016.
3. S. H. Lin and M. H. Liao, "Towards publishing social network data with graph anonymization," *Journal of Intelligent & Fuzzy Systems*, vol. 30, no. 1, pp. 333–345, 2016.
4. C. Zhu et. al., "A Survey on the Integration of Blockchains and Databases," *Data Science and Engineering*, vol. 8, no. 2, pp. 196–219, 2023; doi:10.1007/s41019-023-00212-z
5. K. Liu and E. Terzi, "Towards identity anonymization on graphs," in *Proc. of the 2008 ACM SIGMOD int. conf. on Management of data (SIGMOD '08)*, New York, NY, USA: Association for Computing Machinery, pp. 93–106, 2008; doi:10.1145/1376616.1376629
6. P. Zhang and M. Zhou, "Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, pp. 790–801, 2020; doi:10.1109/tcss.2020.2990103
7. M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication" in *Lecture Notes in Computer Science*, Cham: Springer International Publishing, pp. 112–125, 2016; doi: 10.1007/978-3-319-39028-4_9
8. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering: design principles and practical applications*, Hoboken, NJ, U.S: John Wiley & Sons, 2011.
9. L. Lamport, R. Shostak, M. Pease, "Cryptography Engineering: Design Principles and Practical Applications," in *The Byzantine Generals Problem ACM Transactions on Programming Lanuages and Systems*, Hoboken, NJ, U.S: John Wiley & Sons, vol. 4, no. 3, pp. 382–401, 1982.
10. M. Castro et al., "Practical byzantine fault tolerance," *OsDI*, vol. 99, no. 1999, pp. 173–186, 1999.
11. R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," in *Cryptology ePrint Archive*, 2016. [Online]. Available: https://eprint.iacr.org/2016/917
12. A. Bogdanov et al., "Testing and Comparative Analysis of the F-BFT-based DLT Solution," in *Proc. of Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021*, part IV 21, Springer International Publishing, pp. 31–41, 2021.
13. J. Zhou et al., "A Hybrid Consensus Algorithm for Blockchain," in *2019 IEEE 5th Int. Conf. on Computer and Communications (ICCC)*, IEEE publ., 2019.
14. Y. Zhang et al., "A survey on software defined networking with multiple controllers," *Journal of Network and Computer Applications*, vol. 103, pp. 101–118, 2018; doi:10.1016/j.jnca.2017.11.015
15. M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11–29, 2016; doi:10.1016/j.jnca.2016.05.010

Received 22-06-2023, the final version — 17-08-2023.

Nadezhda Shchegoleva, Doctor of Sciences (Tech.), Associate Professor, Professor of the Department of Fundamental Informatics and Distributed Systems, Saint Petersburg State University, n.shchegoleva@spbu.ru

Jasur Kiyamov, Assistant of the Department of Computer Modeling and Processor Systems, Saint Petersburg State University, ✉ z.kiyamov@spbu.ru