

Errors found in distributed protocols

Protocol	Reference	Violation	Counter-example
PBFT ¹	[CL99]	liveness	[BRB21]
Chord	[Sto+01; LBK02]	liveness ²	[Zav12; Zav17]
Pastry	[RD01]	safety	[AMW16; AMW18]
Generalised Paxos	[Lam05]	non-triviality ³	[SS10]
FaB Paxos	[MA05; MA06]	liveness	[Abr+17]
Multi-Paxos ⁴	[CGR07]	safety	[Mic+17]
Zyzyva	[Kot+07; Kot+10]	safety	[Abr+17]
CRAQ	[TF09]	safety ⁵	[Whi20]
JPaxos	[Koń+11]	safety	[Mic+17]
VR Revisited	[LC12]	safety	[Mic+17]
EPaxos	[MAK13]	safety	[Sut20]
EPaxos	[MAK13]	safety	[Whi21]
Raft	[OO14]	liveness ⁶	[Hoc14]
Raft	[Ong14]	safety ⁷	[AZ15; Ong15]
Raft	[OO14; Ong14]	liveness	[HA20; JHM21]
hBFT	[DPL15]	safety	[SKD19]
Tendermint	[Buc16]	liveness	[CV17]
CAESAR	[Aru+17]	liveness	[Ene+21]
DPaxos	[NAE18]	safety	[Whi+21]
Sync HotStuff	[Abr+19]	safety & liveness	[MC19]
Gasper	[But+20]	safety & liveness	[NTT21]
STM	[IR10]	safety & liveness	[Bel10]

¹With the read-only optimisation.

²Eventual reachability is Chord's key correctness property.

³Acceptors might accept commands that have not been proposed.

⁴As described in Paxos Made Live.

⁵Client reads might fail due to incorrect garbage collection.

⁶The joint consensus membership change algorithm described in the paper version of Raft had a liveness bug, which was fixed in Ongaro's PhD thesis.

⁷The bug is in the single-server membership change scheme described in Ongaro's thesis.

Список литературы

- [Abr+17] Ittai Abraham и др. “Revisiting Fast Practical Byzantine Fault Tolerance”. В: *arXiv:1712.01367 [cs]* (дек. 2017). arXiv: 1712.01367. URL: <http://arxiv.org/abs/1712.01367> (дата обр. 2021-09-06).
- [Abr+19] Ittai Abraham и др. *Sync HotStuff: Simple and Practical Synchronous State Machine Replication*. Тех. отч. 270. 2019. URL: <http://eprint.iacr.org/2019/270> (дата обр. 2021-09-16).
- [AZ15] Brandon Amos и Huanchen Zhang. *15-812 Term Paper: Specifying and proving cluster membership for the Raft distributed consensus algorithm*. Тех. отч. 2015, с. 46. URL: <https://www.cs.cmu.edu/~aplatzer/course/pls15/projects/bamos.pdf>.
- [Aru+17] Balaji Arun и др. “Speeding up Consensus by Chasing Fast Decisions”. В: *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. ISSN: 2158-3927. Июнь 2017, с. 49—60. DOI: 10.1109/DSN.2017.35.
- [AMW16] Noran Azmy, Stephan Merz и Christoph Weidenbach. “A Rigorous Correctness Proof for Pastry”. en. В: *Abstract State Machines, Alloy, B, TLA, VDM, and Z*. Под ред. Michael Butler и др. Т. 9675. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, с. 86—101. ISBN: 978-3-319-33599-5 978-3-319-33600-8. DOI: 10.1007/978-3-319-33600-8_5. URL: http://link.springer.com/10.1007/978-3-319-33600-8_5 (дата обр. 2021-09-07).
- [AMW18] Noran Azmy, Stephan Merz и Christoph Weidenbach. “A machine-checked correctness proof for Pastry”. en. В: *Science of Computer Programming* 158 (июнь 2018), с. 64—80. ISSN: 01676423. DOI: 10.1016/j.scico.2017.08.003. URL: <https://linkinghub.elsevier.com/retrieve/pii/S0167642317301612> (дата обр. 2021-09-07).
- [BRB21] Christian Berger, Hans P. Reiser и Alysson Bessani. “Making Reads in BFT State Machine Replication Fast, Linearizable, and Live”. В: *arXiv:2107.11144 [cs]* (июль 2021). arXiv: 2107.11144. URL: <http://arxiv.org/abs/2107.11144> (дата обр. 2021-11-10).
- [Buc16] Ethan Buchman. “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains”. Дис. . . . док. Guelph, Ontario, Canada: University of Guelph, июнь 2016. URL: <https://atrium.lib.uoguelph.ca/xmlui/handle/10214/9769>.
- [But+20] Vitalik Buterin и др. “Combining GHOST and Casper”. В: *arXiv:2003.03052 [cs]* (май 2020). arXiv: 2003.03052. URL: <http://arxiv.org/abs/2003.03052> (дата обр. 2021-09-16).
- [CV17] Christian Cachin и Marko Vukolić. “Blockchain Consensus Protocols in the Wild”. В: *arXiv:1707.01873 [cs]* (июль 2017). arXiv: 1707.01873. URL: <http://arxiv.org/abs/1707.01873> (дата обр. 2021-09-16).

- [CL99] Miguel Castro и Barbara Liskov. “Practical Byzantine Fault Tolerance”. В: *3rd Symposium on Operating Systems Design and Implementation (OSDI 99)*. New Orleans, LA: USENIX Association, февр. 1999. URL: <https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance>.
- [CGR07] Tushar D. Chandra, Robert Griesemer и Joshua Redstone. “Paxos made live: an engineering perspective”. en. В: *Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing - PODC '07*. Portland, Oregon, USA: ACM Press, 2007, с. 398—407. ISBN: 978-1-59593-616-5. DOI: 10.1145/1281100.1281103. URL: <http://dl.acm.org/citation.cfm?doid=1281100.1281103> (дата обр. 2021-01-19).
- [DPL15] Sisi Duan, Sean Peisert и Karl N. Levitt. “hBFT: Speculative Byzantine Fault Tolerance with Minimum Cost”. В: *IEEE Transactions on Dependable and Secure Computing* 12.1 (январь. 2015). Conference Name: IEEE Transactions on Dependable and Secure Computing, с. 58—70. ISSN: 1941-0018. DOI: 10.1109/TDSC.2014.2312331.
- [Ene+21] Vitor Enes и др. “Efficient replication via timestamp stability”. en. В: *Proceedings of the Sixteenth European Conference on Computer Systems*. Online Event United Kingdom: ACM, апр. 2021, с. 178—193. ISBN: 978-1-4503-8334-9. DOI: 10.1145/3447786.3456236. URL: <https://dl.acm.org/doi/10.1145/3447786.3456236> (дата обр. 2021-09-16).
- [Hoc14] Ezra Hoch. *Configuration changes*. Февр. 2014. URL: https://groups.google.com/g/raft-dev/c/xux5HRxH3Ic/m/mz_PDK-qMJgJ (дата обр. 2021-09-09).
- [HA20] Heidi Howard и Ittai Abraham. *Raft does not Guarantee Liveness in the face of Network Faults*. Дек. 2020. URL: <https://decentralizedthoughts.github.io/2020-12-12-raft-liveness-full-omission/> (дата обр. 2021-05-07).
- [IR10] Damien Imbs и Michel Raynal. “Software transactional memories: an approach for multicore programming”. В: *The Journal of Supercomputing*. DOI: <https://doi.org/10.1007/s11227-010-0388-0>. Февр. 2010.
- [JHM21] Chris Jensen, Heidi Howard и Richard Mortier. “Examining Raft’s behaviour during partial network failures”. В: *Proceedings of the 1st Workshop on High Availability and Observability of Cloud Systems*. HAOC ’21. New York, NY, USA: Association for Computing Machinery, апр. 2021, с. 11—17. ISBN: 978-1-4503-8336-3. DOI: 10.1145/3447851.3458739. URL: <https://doi.org/10.1145/3447851.3458739>.
- [Koń+11] Jan Kończak и др. *JPaxos: State machine replication based on the Paxos protocol*. Тех. отч. EPFL-REPORT-167765. 2011.

- [Kot+07] Ramakrishna Kotla и др. “Zyzyva: Speculative Byzantine Fault Tolerance”. В: *SIGOPS Oper. Syst. Rev.* 41.6 (окт. 2007), с. 45—58. ISSN: 0163-5980. DOI: 10.1145/1323293.1294267. URL: <https://doi.org/10.1145/1323293.1294267>.
- [Kot+10] Ramakrishna Kotla и др. “Zyzyva: Speculative Byzantine Fault Tolerance”. В: *ACM Trans. Comput. Syst.* 27.4 (январь. 2010). ISSN: 0734-2071. DOI: 10.1145/1658357.1658358. URL: <https://doi.org/10.1145/1658357.1658358>.
- [Lam05] Leslie Lamport. *Generalized Consensus and Paxos*. Тех. отч. MSR-TR-2005-33. Microsoft Research, март 2005. URL: <https://www.microsoft.com/en-us/research/publication/generalized-consensus-and-paxos/>.
- [LBK02] David Liben-Nowell, Hari Balakrishnan и David Karger. “Analysis of the Evolution of Peer-to-Peer Systems”. В: *Proceedings of the Twenty-First Annual Symposium on Principles of Distributed Computing*. PODC ’02. Monterey, California: Association for Computing Machinery, 2002, с. 233—242. ISBN: 1581134851. DOI: 10.1145/571825.571863. URL: <https://doi.org/10.1145/571825.571863>.
- [LC12] Barbara Liskov и James Cowling. *Viewstamped Replication Revisited*. ен. Тех. отч. MIT-CSAIL-TR-2012-021. Июль 2012, с. 16.
- [MA05] J.-P. Martin и L. Alvisi. “Fast Byzantine Consensus”. В: *2005 International Conference on Dependable Systems and Networks (DSN’05)*. ISSN: 2158-3927. Июнь 2005, с. 402—411. DOI: 10.1109/DSN.2005.48.
- [MA06] Jean-Philippe Martin и Lorenzo Alvisi. “Fast Byzantine Consensus”. English. В: *IEEE Transactions on Dependable and Secure Computing* 3.3 (сентябрь. 2006). Num Pages: 202-215 Place: Washington, United States Publisher: IEEE Computer Society, с. 202—215. ISSN: 15455971. DOI: <http://dx.doi.org.libproxy1.nus.edu.sg/10.1109/TDSC.2006.35>. URL: <http://www.proquest.com/docview/206534931/abstract/A91EECC1018D4A46PQ/1>.
- [Mic+17] Ellis Michael и др. “Recovering Shared Objects Without Stable Storage”. ен. В: (авг. 2017). Appendix B, с. 27.
- [MC19] Atsuki Momose и Jason Paul Cruz. *Force-Locking Attack on Sync Hotstuff*. Тех. отч. 1484. 2019. URL: <http://eprint.iacr.org/2019/1484> (дата обр. 2021-09-16).
- [MAK13] Iulian Moraru, David G. Andersen и Michael Kaminsky. “There is more consensus in Egalitarian parliaments”. В: *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*. SOSR ’13. New York, NY, USA: Association for Computing Machinery, ноябрь. 2013, с. 358—372. ISBN: 978-1-4503-2388-8. DOI: 10.1145/2517349.2517350. URL: <http://doi.org/10.1145/2517349.2517350>.

- [NAE18] Faisal Nawab, Divyakant Agrawal и Amr El Abbadi. “DPaxos: Managing Data Closer to Users for Low-Latency and Mobile Applications”. В: *Proceedings of the 2018 International Conference on Management of Data*. SIGMOD ’18. New York, NY, USA: Association for Computing Machinery, май 2018, с. 1221—1236. ISBN: 978-1-4503-4703-7. DOI: 10.1145/3183713.3196928. URL: <https://doi.org/10.1145/3183713.3196928> (дата обр. 2021-09-07).
- [NTT21] Joachim Neu, Ertem Nusret Tas и David Tse. “Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma”. В: *arXiv:2009.04987 [cs]* (февр. 2021). arXiv: 2009.04987. URL: <http://arxiv.org/abs/2009.04987> (дата обр. 2021-09-16).
- [Ong14] Diego Ongaro. “Consensus: Bridging Theory and Practice”. AAI28121474. Дис. ... док. Stanford, CA, USA, 2014. ISBN: 9798662514218.
- [Ong15] Diego Ongaro. *bug in single-server membership changes*. Июль 2015. URL: <https://groups.google.com/g/raft-dev/c/t4xj6dJTP6E/m/d2D9LrWRza8J> (дата обр. 2021-09-01).
- [OO14] Diego Ongaro и John Ousterhout. “In Search of an Understandable Consensus Algorithm”. В: *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference*. USENIX ATC’14. Philadelphia, PA: USENIX Association, 2014, с. 305—320. ISBN: 9781931971102.
- [RD01] Antony Rowstron и Peter Druschel. “Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems”. en. В: *Middleware 2001*. Под ред. Rachid Guerraoui. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001, с. 329—350. ISBN: 978-3-540-45518-9. DOI: 10.1007/3-540-45518-3_18.
- [SKD19] Nibesh Shrestha, Mohan Kumar и SiSi Duan. “Revisiting hBFT: Speculative Byzantine Fault Tolerance with Minimum Cost”. В: *arXiv:1902.08505 [cs]* (апр. 2019). arXiv: 1902.08505. URL: <http://arxiv.org/abs/1902.08505> (дата обр. 2021-09-16).
- [Sto+01] Ion Stoica и др. “Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications”. В: *SIGCOMM Comput. Commun. Rev.* 31.4 (авг. 2001), с. 149—160. ISSN: 0146-4833. DOI: 10.1145/964723.383071. URL: <https://doi.org/10.1145/964723.383071>.
- [Sut20] Pierre Sutra. “On the correctness of Egalitarian Paxos”. en. В: *Information Processing Letters* 156 (апр. 2020). ISSN: 0020-0190. DOI: 10.1016/j.ipl.2019.105901. URL: <https://www.sciencedirect.com/science/article/pii/S002001901930184X> (дата обр. 2021-04-01).
- [SS10] Pierre Sutra и Marc Shapiro. *Fast Genuine Generalized Consensus*. Tex. отч. (corrected August 2010). Section 6.3. Февр. 2010, с. 62. URL: <https://drive.google.com/open?id=0BwFkGepvBDQoRjNYRGJTdWQ0SZA>.

- [TF09] Jeff Terrace и Michael J. Freedman. “Object Storage on {CRAQ}: High-Throughput Chain Replication for Read-Mostly Workloads”. В: 2009. URL: <https://www.usenix.org/conference/usenix-09/object-storage-craq-high-throughput-chain-replication-read-mostly-workloads> (дата обр. 2021-09-09).
- [Whi20] Michael Whittaker. “CRAQ Bug”. original-date: 2020-06-13T18:44:33Z. Июнь 2020. URL: https://github.com/mwhittaker/craq_bug (дата обр. 2021-09-09).
- [Whi21] Michael Whittaker. *EPaxos Dependency Set Compaction Bug*. original-date: 2018-11-03T04:31:20Z. Сент. 2021. URL: https://github.com/mwhittaker/bipartisan_paxos/blob/cbd99cc735215d18c163dc41cb0a05edcb55437d/epaxos_bugs/epaxos_dependency_bug.pdf (дата обр. 2021-09-16).
- [Whi+21] Michael Whittaker и др. “Matchmaker Paxos: A Reconfigurable Consensus Protocol”. en. В: *Journal of Systems Research* (2021), с. 22.
- [Zav12] Pamela Zave. “Using lightweight modeling to understand chord”. en. В: *ACM SIGCOMM Computer Communication Review* 42.2 (март 2012), с. 49—57. ISSN: 0146-4833. DOI: 10.1145/2185376.2185383. URL: <https://dl.acm.org/doi/10.1145/2185376.2185383> (дата обр. 2021-09-06).
- [Zav17] Pamela Zave. “Reasoning About Identifier Spaces: How to Make Chord Correct”. В: *IEEE Transactions on Software Engineering* 43.12 (дек. 2017). Conference Name: IEEE Transactions on Software Engineering, с. 1144—1156. ISSN: 1939-3520. DOI: 10.1109/TSE.2017.2655056.
- [Бел10] Беляев. “Верификация алгоритма поддержки транзакционной памяти”. В: *Информатика, телекоммуникации и управление. 2010. №3 (101)*. Февр. 2010. URL: <https://cyberleninka.ru/article/n/verifikatsiya-algoritma-podderzhki-tranzaktsionnoy-pamyati>.