BFT Consensus: From Academic Paper to Mainnet

Alberto Sonnino
Mysten Labs, London, UK
University College London (UCL), UK

Abstract

This talk shares our journey in bringing Byzantine Fault Tolerant (BFT) consensus from academic papers to operational blockchain networks. It begins in 2019 with our initial effort as researchers and engineers at Facebook to deploy the HotStuff consensus protocol [12] at the heart of the Libra blockchain [5]. We present how this journey led to modifications from the original theoretical design [6] and the eventual migration to DAG-based systems [4, 10], now implemented in the Sui blockchain [11] and gaining traction across the blockchain space [1, 2, 9, 8]. We outline the numerous research and engineering challenges we faced at every step of this journey, describe how we addressed some of these challenges [3, 7], and point out which ones remain open questions and require further research. This talk aims to offer a different perspective on BFT consensus, focusing on the needs of real-world blockchains and offering insights that may not be visible from research papers alone.

2012 ACM Subject Classification Security and privacy → Distributed systems security

Keywords and phrases BFT Consensus, Blockchain, Real-World

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2024.3

Category Invited Talk

References

1. Balaji Arun, Zekun Li, Florian Suri-Payer, Sourav Das, and Alexander Spiegelman. Shoal++: High throughput dag bft can be fast! *arXiv preprint*, 2024. doi:10.48550/arXiv.2405.20488.
2. Kushal Babel, Andrey Chursin, George Danezis, Lefteris Kokoris-Kogias, and Alberto Sonnino. Mysticeti: Low-latency dag consensus with fast commit path, 2024. arXiv:2310.14821.
3. Shehar Bano, Alberto Sonnino, Andrey Chursin, Dmitri Perelman, Zekun Li, Avery Ching, and Dahlia Malkhi. Twins: Bft systems made robust. *arXiv preprint*, 2020. arXiv:2004.10617.
4. George Danezis, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. Bridging the gap of timing assumptions in byzantine consensus. In *EuroSys '22: Proceedings of the Seventeenth European Conference on Computer Systems*, 2022. doi:10.1145/3590140.3629114.
5. Facebook. Welcome to the diem project. https://www.diem.com/en-us/, 2022.
6. Rati Gelashvili, Lefteris Kokoris-Kogias, Alberto Sonnino, Alexander Spiegelman, and Zhuolun Xiang. Jolteon and ditto: Network-adaptive efficient consensus with asynchronous fallback, 2021. arXiv:2106.10362.
7. Giacomo Giuliari, Alberto Sonnino, Marc Frei, Fabio Streun, Lefteris Kokoris-Kogias, and Adrian Perrig. An empirical study of consensus protocols' dos resilience. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 2024.
8. Dahlia Malkhi, Chrysoula Stathakopoulou, and Maofan Yin. Bbca-chain: One-message, low latency bft consensus on a dag. *arXiv preprint*, 2023. doi:10.48550/arXiv.2310.06335.
9. Nibesh Shrestha, Rohan Shrothrium, Aniket Kate, and Kartik Nayak. Sailfish: Towards improving latency of dag-based bft. *Cryptology ePrint Archive*, 2024.
10. Alexander Spiegelman, Neil Giridharan, Alberto Sonnino, and Lefteris Kokoris-Kogias. Bullshark: Dag bft protocols made practical. In *CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022. doi:10.1145/3548606.3559361.
11. The Sui team. The sui blockchain, 2023. URL: http://sui.io.
12. Maofan Yin, Dahlia Malkhi, Michael K Reiter, Guy Golan Gueta, and Ittai Abraham. Hotstuff: Bft consensus with linearity and responsiveness. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, pages 347–356, 2019. doi:10.1145/3293611.3331591.