Evaluating Blockchain Fault Tolerance with STABL

Vincent Gramoli
University of Sydney and Redbelly Network
Australia
vincent.gramoli@sydney.edu.au

Rachid Guerraoui
EPFL
Switzerland
rachid.guerraoui@epfl.ch

Andrei Lebedev
University of Sydney
Australia
andrei.lebedev@sydney.edu.au

Gauthier Voron
EPFL
Switzerland
gauthier.voron@epfl.ch

***Abstract*—Despite their distributed nature, blockchains frequently experience failures that disrupt availability, delay transactions, and, in some cases, cause total network outages. Ensuring fault tolerance is critical for the reliability of blockchain-based applications, yet existing evaluations often overlook real-world failure scenarios. Assessing dependability requires systematic fault injection and measurement techniques to understand how different blockchains handle crashes, network partitions, and Byzantine failures. This tutorial dives into the details of using STABL, a benchmark suite to evaluate blockchains behavior in the presence of faulty processes, understanding the results, and extending the implementation to support a new fault type, providing attendees with a hands-on approach to blockchain fault tolerance evaluation.**

***Index Terms*—Reliability, measurement techniques, fault injection, distributed systems, performance measures.**

I. Overview

Blockchains are often assumed to be fault tolerant due to their decentralized nature, yet real-world failures repeatedly challenge this assumption. Outages lasting days have been observed across major blockchain networks [1]. Some could not even recover from transient isolated failures [2]. Unlike traditional distributed systems, where well-established fault tolerance mechanisms exist, blockchains vary significantly in their consensus protocols, network structures, and failure handling approaches, making dependability evaluation particularly challenging. Despite the critical importance of fault tolerance, most blockchain benchmarking efforts focus primarily on performance metrics such as throughput and latency, often under ideal conditions that fail to account for real-world failure scenarios [3].

Evaluating fault tolerance requires a systematic approach to fault injection and measurement, enabling researchers and practitioners to analyze blockchain resilience, recoverability, and failure impact. This tutorial focuses on dependability assessment, covering practical methods for introducing faults, observing their effects, and quantifying blockchain sensitivity to failures, providing a different perspectives on blockchain performance evaluation compared to our tutorial on performance benchmarking with DIABLO [4].

In this *half-day* tutorial, we will evaluate the fault tolerance of one of the six blockchains, Algorand [5], Avalanche [6], Aptos [7], Ethereum [8], Redbelly [9] and Solana [10] with the recent STABL [2] benchmark suite. We will look at the sensitivity score and extend the observer node with another fault type.

The tutorial will have the following structure:

- **Introduction** (20 min). What is blockchain, transaction throughput and latency, DIABLO and STABL benchmarking frameworks.
- **Simple Demo** (30 min). Using the virual machine image, members of the audience will run a local experiment on their own machines.
- **Fault Tolerance and Dependability** (20 min). Explanation of crash faults and network partitioning, and packet loss.
- **Fault Tolerance Demo** (30 min). We will introduce crash faults in the scenario and observe performance and sensitivity score under new conditions.
- **Benchmarking Details** (20 min). Explanation of metrics, workload types, and emulating various network conditions.
- **Advanced Demo** (30 min). We will explain the fault scenario implementation in STABL observer node and how to extend it with a new fault type.
- **Discussion** (30 min). Implications of design decisions, metrics and aspects to be evaluated.

II. Objectives

The goal of the tutorial is to spark the interest of the community in blockchain fault tolerance evaluation. We aim at easing the entry to the subject by providing simple hands-on experience.

The main objectives of this tutorial are to:

- Provide an in-depth understanding of blockchain fault tolerance.
- Demonstrate fault injection and analysis capabilities of STABL.
- Enable participants to extend STABL with a new failure model.

III. Supporting Material and Target Audience

To complement the tutorial content with practical resources, we provide slides, a virtual machine image containing the required software and scenarios to demonstrate fault tolerance evaluation, and the project website[1].

The tutorial is aimed for general audience interested in blockchains, and dependability and reliability analysis, as well as specialists in the field. We will cover both the basic aspects,

[1] https://diablobench.github.io

potential pitfalls and future work directions in blockchain fault tolerance evaluation.

Acknowledgment

This work is supported in part by the Australian Research Council Discovery Project funding scheme (#250101739).

References

[1] Eddie Mitchell, "Solana Outage: Full List Of SOL Network Blockchain Mainnet Failures," https://cryptomaniaks.com/crypto-news/solana-outage-list-failures-sol-blockchain-mainnet, 2024, accessed on 31 Aug. 2024.

[2] V. Gramoli, R. Guerraoui, A. Lebedev, and G. Voron, "Stabl: Blockchain fault tolerance," arXiv, Tech. Rep. 2409.13142, 2024.

[3] V. Gramoli, R. Guerraoui, A. Lebedev, C. Natoli, and G. Voron, "Diablo: A benchmark suite for blockchains," in *Proceedings of the Eighteenth European Conference on Computer Systems*, ser. EuroSys '23, 2023. [Online]. Available: https://doi.org/10.1145/3552326.3567482

[4] A. Lebedev and V. Gramoli, "Evaluating performance and dependability of blockchain protocols with diablo," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, 2024, pp. 69–70.

[5] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Principles (SOSP)*. ACM, 2017, pp. 51–68.

[6] T. Rocket, M. Yin, K. Sekniqi, R. van Renesse, and E. G. Sirer, "Scalable and probabilistic leaderless BFT consensus through metastability," arXiv, Tech. Rep., Aug. 2020. [Online]. Available: http://arxiv.org/abs/1906.08936

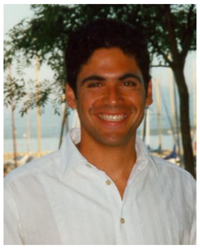
[7] (2022, Aug.) The Aptos blockchain: Safe, scalable, and upgradeable Web3 infrastructure. Accessed: Aug. 31, 2024. [Online]. Available: https://aptosfoundation.org/whitepaper/aptos-whitepaper_en.pdf

[8] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2015, yellow paper.

[9] T. Crain, C. Natoli, and V. Gramoli, "Red Belly: a secure, fair and scalable open blockchain," in *Proc. 42nd IEEE Symp. Security and Privacy (S&P)*, May 2021.

[10] A. Yakovenko. (2021) Solana: A new architecture for a high performance blockchain v0.8.13. Accessed: Aug. 31, 2024. [Online]. Available: https://solana.com/solana-whitepaper.pdf

Vincent Gramoli is a Professor of Computer Science at the University of Syndey and the Founder and CTO of Redbelly Network. He received the Digital National Facilities & Collections Award from CSIRO, the Education Leader of the Year Award from Blockchain Australia, and the Future Fellowship from the Australian Research Council. In the past, Vincent Gramoli has been affiliated with INRIA, Cornell, Data61 and EPFL.



Rachid Guerraoui is a professor with the Ecole Polytechnique Fédérale de Lausanne (EPFL) where he leads the Distributed Computing Laboratory. He has been affiliated with the Research Center of Ecole des Mines de Paris, the Commissariat a l'Energie Atomique in Saclay, Hewlett-Packard Laboratories in Palo Alto and the Massachusetts Institute of Technology. His research is devoted to concurrent and distributed computing, from multiprocessors to wide-area networks.

Andrei Lebedev is a PhD student at the University of Sydney. The focus of his research is evaluation and improvement of distributed systems. He received his MSc in Informatics from the Technical University of Munich and has been a technical lead for Hyperledger Iroha, a permissioned blockchain protocol. He served as Artifact Evaluation Committee member of international scientific conferences (OSDI'23, USEINX ATC'23).

Gauthier Voron is a postdoctoral researcher in Computer Science at the Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland. He holds a PhD from Sorbonne Université, France, obtained in 2018 for his work on virtualization of Non Uniform Memory Architecture. His research interests revolve around performance and scalability of concurrent and distributed systems with a particular focus on interactions of low level and high level aspects of distributed systems.