MOdular Blockchain Simulator: Talk proposal*

António Ravara
NOVA School of Science and Technology, Portugal

Abstract

MOBS is a simulator and GUI developed with the goal of aiding in the development and study of consensus protocols. It aims to address practical challenges in designing, implementing and maintain-ing (blockchain) consensus protocols by providing a simulation environment and a visualiser to analyse their behaviour, and by offering empirical metrics of their runtime in different environments and conditions. The simulator is parametrized through json files. The GUI offers a way to change the parameterisations without the need of manually changing those files. It also allows the user to specify intervals of possible values for specific parameters. By clicking on Run Simulation, the program produces one json file for each combination of parameter values as well as batches, within the specified intervals, and executes the simulation with each of those parameterisations (which produces outputX-Y.json files, where X is the id assigned to the combination of parameters, and Y is the batch number for that combination).

1 Problem and goals

Consensus protocols are not trivial to define or understand and in blockchain systems, where the behaviour can be dynamic and mostly financial transactions are dealt with, their correctness is crucial and errors can be costly. One example of this is Ethereum moving from Proof of Work to a Proof of Stake consensus; this opened the protocol to vulnerabilities to bouncing attacks on liveness. This type of attack prevents the chain from being finalized because the main selected chain in the fork choice rule is continually bouncing between two alternative branches. There is also Solana, a new blockchain protocol that relies on Proof-of-History to build its chain, where repeated testing results showed that the protocol does not fully achieve consensus and a single malicious validator can halt the Solana blockchain. These tests also showed that there are inconsistencies in the behaviour between what is described in the documentation and what the protocol showed since Solana's implementation has deviated in undocumented ways from the available protocol design descriptions.

Consensus and blockchain protocols are usually described with pseudocode and model checked with idealized languages, what does not reflect the implementations. Since evaluating correctness is very costly, before planing an implementation, developers should test their ideas and prototypes. There is a lack of

*Joint work with Miguel Alves, Marco Giunti, and Simão Melo de Sousa

methodologies to develop, evaluate, tune and replicate these protocols, opening a need for extensible and modular tools for consensus analysis and experimental labs for rapid prototyping. With this in mind MOBS was developed with the aim to give the ability to test and validate these protocols under different conditions and settings by changing the execution parameters, aiming to catch vulnerabilities or even logic errors before deploying changes to these protocols. Since verification of protocols is very costly, developers can use MOBS to get confidence in their implementations from experimentations first.

2 Summary of contribution

This work tackles the lack of configurable and modular experimentation environments to test and assess the behaviour of, and to provide quality assurances on, consensus protocols. MOBS, our web-based software platform, is a general-purpose simulator, coupled with a Web Graphical User Interface (*GUI*), to check the effect of running an instantiation of a protocol, defined by the developer but building on abstractions we provide (thus simplifying coding effort). MOBS is constituted by a simulator and a highly parameterisable GUI that aids in the configuration and analysis of simulations, offering built-in a large set of variables, and being customisable, as a user can define additional fields.

To assess the effectiveness of the MOBS platform, we simulated and tested **thirteen protocols** among classical and blockchain: Chandra-Toueg [CT96], Flooding, Paxos [Lam98], Multi-Paxos and Tenderbake [ACP+20][1]; Algorand [GHM+17], Bitcoin-like PoW (Nakamoto, Dogecoin, and Litecoin), Ethereum +PoW and PoS, Ouroboros Praos [DGKR18], and Ouroboros BFT [KR18]. To the best of our knowledge, no other simulator showcased a similar amount of protocols and tackled both classical and blockchain consensus in the same platform.

The work we present herein was validated by comparing simulated metrics, such as median block propagation times and median round duration, with real-world results. We developed optimisations for the simulation of distributed protocols building on an optional general-purpose abstraction, which can be used under a given set of conditions and leads to significantly faster simulations.

The platform, constituted by the simulator, implemented in OCaml, and the Web GUI, is open-source and publicly available on GitHub under the MIT License.

References

[ACP+20] Lacramioara Astefanoaei, Pierre Chambart, Antonella Del Pozzo, Edward Tate, Sara Tucci Piergiovanni, and Eugen Zalinescu. Tenderbake - classical BFT style consensus for public blockchains. *CoRR*, abs/2001.11965, 2020.

[CT96] Tushar D. Chandra and Sam Toueg. Unreliable failure detectors for reliable distributed systems. *Journal of the ACM (JACM)*, 43(2):225–267, 1996.

[1] Tenderbake is actually a blockchain algorithm, but uses "classical" committee-based BFT consensus.

[DGKR18] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 66–98, Cham, 2018. Springer International Publishing.

[GHM+17] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*, pages 51–68. ACM, 2017.

[KR18] Aggelos Kiayias and Alexander Russell. Ouroboros-bft: A simple byzantine fault tolerant consensus protocol. *IACR Cryptol. ePrint Arch.*, page 1049, 2018.

[Lam98] Leslie Lamport. The part-time parliament. In *ACM Transactions on Computer Systems (TOCS)*, volume 16, pages 133–169, 1998.