Demo: VIBES: Fast Blockchain Simulations for Large-scale Peer-to-Peer Networks

Lyubomir Stoykov[1], Kaiwen Zhang[1,2,3], Hans-Arno Jacobsen[2]
[1]Technical University of Munich
[2]Middleware Systems Research Group
[3]University of Toronto

Abstract

Following the success of Bitcoin, Ethereum and Hyperledger, blockchains are now gaining widespread adoption in a wide variety of applications, using a diversity of distributed ledger systems with varying characteristics. Yet, beyond the original bitcoin protocol, the safety and reliability properties of such systems are not sufficiently analyzed. To better understand the behavior of these systems, we propose VIBES: a configurable blockchain simulator for large scale peer-to-peer networks. With VIBES, users can explore important characteristics and metrics of the network, reason about interactions between nodes, and compare different scenarios in an intuitive way. VIBES differentiates itself from previous works in its ability to simulate blockchain systems beyond bitcoin and its support for large-scale simulations with thousands of nodes.

CCS Concepts • **Networks → Peer-to-peer networks**;

Keywords Blockchain, Simulation

ACM Reference Format:
Lyubomir Stoykov[1], Kaiwen Zhang[1,2,3], Hans-Arno Jacobsen[2]. 2017. Demo: VIBES: Fast Blockchain Simulations for Large-scale Peer-to-Peer Networks. In *Proceedings of Middleware Posters and Demos '17: Proceedings of the Posters and Demos Session of the 18th International Middleware Conference, Las Vegas, NV, USA, December 11–15, 2017 (Middleware Posters and Demos '17),* 3 pages.
https://doi.org/10.1145/3155016.3155020

1 Introduction

We propose *Visualizations of Interactive, Blockchain, Extended Simulations* (VIBES): a configurable blockchain simulator capable of conducting large-scale network simulations in order to derive empirical insights on the behavior of a particular system. VIBES is envisioned as a valuable tool for blockchain end users to develop an intuitive understanding of the behavior of their system. To this end, the simulator achieves two objectives: scalability and speed. Scalability refers to the ability to simulate large networks with thousands of nodes, which provide deeper insights on deployed systems. Speed is important since fast simulation results allow the end user to interact with VIBES by adjusting parameters until the desired outcomes are achieved. We demonstrate the features of our simulator VIBES using an interactive demo.

Middleware Posters and Demos '17, December 11–15, 2017, Las Vegas, NV, USA

ACM ISBN 978-1-4503-5201-7/17/12.
https://doi.org/10.1145/3155016.3155020

2 Related works

Previous attempts have recently been made to explore different properties of distributed ledgers, particularly cryptocurrency [1, 3, 4]. A first type of approach *performs a back-of-the envelope calculation* using empirical data to infer certain properties of the network [2]. The benefit of this approach lies in the analysis of very large networks without heavy computations. However, this approach is not general, since it usually explore a single-case scenario, where parameters correspond to the real-world configuration of the network.

In a second approach, a simulator bootstraps an entire peer-to-peer network in a test environment where parameters (e.g., number of nodes, network bandwidth) are specified by the user [3, 4]. Since these works span entire networks with close-to-real nodes, sockets, and mining, this approach results in heavy-handed simulations, which cannot scale beyond a hundred nodes.

To the best of our knowledge, no tool exists which can analyze performance and security properties of a generic blockchain network. As a result, it is difficult to predict the behaviour of distributed ledgers, proven by the fact that developers hardly settle on any new proposals to improve existing implementations [6]. Our simulator addresses this painpoint and is directed towards heavy blockchain users, companies, and developers looking to make an educated decision, identify bottlenecks, and improve applications of blockchains and their underlying algorithms and protocols.

3 Proposed solution

Figure 1 depicts the VIBES architecture. After a browser client sends input parameters to the web server, the orchestrator bootstraps the desired amount of nodes, configures them, and starts the simulation.

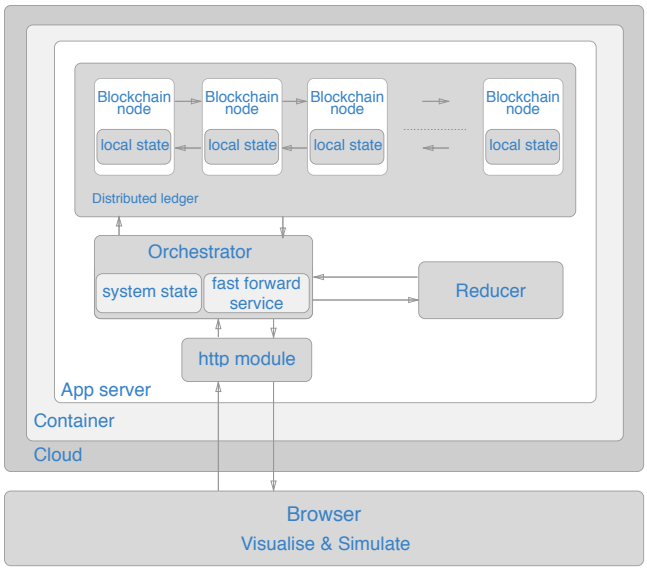

Figure 1. VIBES Architecture

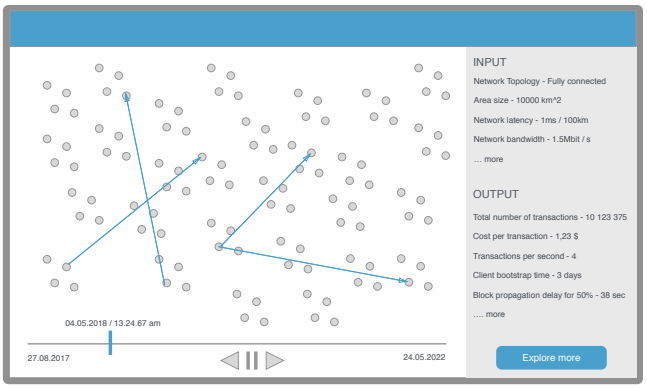

Figure 2. VIBES Web Client

VIBES addresses the flexibility issues of previous approaches via configurable input parameters. Input parameters include: network topology, area size, latency, bandwidth, number of nodes, number of miners, block size, block confirmation time, number of transactions per block / transaction size, electricity cost, smart contract time, smart contract intensity and smart contract density, percentage of attacker nodes, percentage of failing nodes. The simulator outputs the following metrics: total time to process, total number of transactions processed, throughput (transactions per second), block propagation delay for 10%, 50% and 90%, client bootstrap time, cost per transaction, probability of an attacker taking over at each stage, and a log of all transactions.

To improve scalability, we propose the concept of fast-forward computing. Using relevant input parameters coupled with empirical and theoretical results, the application is able to skip most of the heavy computations and simulate ahead of time at a large scale. Nodes can calculate how much a potential operation would take and ask the orchestrator for permission to fast-forward. If there are no conflicts, the orchestrator issues a timestamp for this operation, labels it as complete, notifies the whole network and skips ahead to the point in time carried by the timestamp. After nodes have finished their work, the reducer receives the global state carried by the orchestrator, which includes timestamped transactions. The reducer then applies a stateless function on the data and delivers the response to the browser client. The web client then has structured and labeled data and is therefore able to give powerful insights to the user and also simulate the interaction between nodes in an intuitive fashion via a *time-lapse* (see Figure 2).

The following example illustrates the concept of fast-forwarding. For instance, suppose we wish to simulate a blockchain system where miners resolve consensus using Proof-of-Work, using a block time of 10 minutes like bitcoin [5]. Without fast-forwarding, a simulation would require 10 minutes to insert each block. Instead, VIBES applies fast-forwarding in the following manner: each node makes a best guess on the time to complete the operation, then sends this information to the orchestrator, and asks for permission to skip ahead and label the block as mined. The orchestrator then waits until it receives this information from every node and retains the earliest timestamp ts (to finish Proof-of-Work) received. The orchestrator gives permission to the node with the earliest timestamp ts to mine the block, assigns ts as the time of the mining operation, and fast-forwards the entire network to time ts. All nodes reset their best guesses and continue with the next operation in their stack. The system works recursively until nodes have finished their work.

4 Acknowledgements

Supported by Alexander von Humboldt Foundation. We thank Richard Hull (IBM) for discussions on Hyperledger.

References

[1] BlockExplorer. 2014. Bitcoin block explorer simulator. https://blockexplorer.com/. (2014). Accessed: 2017-08-30.

[2] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. 2016. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer, 106–125.

[3] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan. 2017. BLOCKBENCH: A Framework for Analyzing Private Blockchains. *ArXiv e-prints* (March 2017). arXiv:cs.DB/1703.04057

[4] Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the Security and Performance of Proof of Work Blockchains. In *Proceedings of the 23nd ACM SIGSAC Conference on Computer and Communication Security (CCS)*. ACM.

[5] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

[6] veleslavs. 2017. Bitcoin improvement proposal. https://github.com/bitcoin/bips/pull/555. (2017). Accessed: 2017-09-08.