Research Internship : Peer Selection in Gossip-Based Blockchain

1 Supervision

Advisers	François Taiani, `francois.tainai@irisa.fr`, 02 99 84 75 04
	Davide Frey, `davide.frey@inria.fr`
	Amaury Bouchra-Pilet, `Amaury.Bouchra-Pilet@irisa.fr`
Lab	Centre Inria Rennes, IRISA (UMR 6074)
Team	WIDE (The World Is DistributEd)
	Équipes-Projet Inria / Département D1 IRISA

2 Context

Since the introduction of Bitcoin [8], blockchain platforms have attracted enormous interest from the general public, government, the industry, and the research community. A number of actors have thus proposed a variety of alternative solutions either introducing new features [11] or improving on aspects such as privacy [2], or computational cost [1, 10, 9, 5]. In particular, in the context of unpermissioned blockchains—those with an open and unknown-a-priori set of participants—a number of authors have proposed solutions based on randomized protocols [9, 5] for disseminating updates and achieving consensus. In this context, Avalanche [9] promises a blockchain that can scale to very large networks with minimal cost. Yet, the current Avalanche proposal relies on network nodes' maintaining a complete graph, which raises scalability issues.

3 Objective

The goal of this research internship lies in exploring how protocols like Avalanche [9] perform when the assumption of a complete graph is not satisfied. In particular, we plan to consider gossip-based peer-sampling protocols [6], which provide nodes with a continuously changing random sample of the network, as well as variants that provide protection against attackers [3, 4].

4 Tasks

- The first task will consist in implementing a simulator for the Avalanche protocol and testing it in a number of settings where the complete-graph assumption is not satisfied.
- In a second step, we will test Avalanche in combination with a well-known gossip-based peer-sampling protocol [7] and in situations where this peer-sampling can be biased by an attacker.
- Finally, the internship will seek to solve the issues identified in the first two tasks by applying an existing attack-resilient peer-sampling protocol [4].

5 Candidate Profile

In this internship, the student is expected to be proficient in Object-Oriented Programming and able to understand C++ code. The student will also be familiar and at ease with at least basic probability theory.

References

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco, and Jason Yellick. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, April 23-26, 2018*, pages 30:1–30:15, 2018.

[2] Eli Ben-sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. pages 459–474, 05 2014.

[3] Edward Bortnikov, Maxim Gurevich, Idit Keidar, Gabriel Kliot, and Alexander Shraer. Brahms: Byzantine resilient random membership sampling. *Computer Networks*, 53(13):2340–2359, 2009.

[4] Amaury Bouchra-Pilet. Robust privacy-preserving gossip averaging. Master's thesis, ENS Ulm - Inria Rennes, 2018. `https://github.com/ALRBP/Private_Gossip_Average/blob/master/report.pdf`.

[5] 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*, SOSP '17, pages 51–68, New York, NY, USA, 2017. ACM.

[6] Márk Jelasity, Spyros Voulgaris, Rachid Guerraoui, Anne-Marie Kermarrec, and Maarten van Steen. Gossip-based peer sampling. *ACM TOCS*, 25, 2007.

[7] Márk Jelasity, Spyros Voulgaris, Rachid Guerraoui, Anne-Marie Kermarrec, and Maarten Van Steen. Gossip-based peer sampling. *ACM ToCS*, 25(3):8, 2007.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[9] Team Rocket. Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies, May 2018.

[10] Marko Vukolic. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*, pages 112–125, 2015.

[11] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger, 2014. http://bitcoinaffiliatelist.com/wp-content/uploads/ethereum.pdf (accessed April 3rd, 2018).