M2/Final Year Engineering Internship: Novel Blockchain-inspired Fault-Tolerance and Sybil-protection techniques for P2P storage

Context

Hive (https://www.hivenet.com/), a young and dynamic startup, is collaborating with the WIDE (https://team.inria.fr/wide/) and COAST (https://team.inria.fr/coast/) Inria teams on Byantine-tolerant P2P storage, and is offering a 6-months research and development internship for final year CSc students on these topics. The intern will will be located at the Hive offices in Cannes.

About Hive:

Hive intends to play the role of a next generation cloud provider in the context of Web 3.0. Hive aims to exploit the unused capacity of computers to offer the general public a greener and more sovereign alternative to the existing clouds where the true power lies in the hands of the users. It relies both on distributed peer-to-peer networks, on the encryption of end-to-end data and on blockchain technology.

About Inria Center of the University of Rennes:

The Inria Center of the University of Rennes is one of Inria's eight centers and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institutes, etc.

About Inria Nancy - Grand Est:

The Inria Nancy - Grand Est center is one of Inria's eight centers and has twenty project teams, located in Nancy, Strasbourg and Saarbrücken. Its activities occupy over 400 people, scientists and research and innovation support staff, including 45 different nationalities. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institutes, etc.

Objective

A key challenge in a distributed storage system lies is withstanding the behavior of Byzantine nodes. These can result from malicious actors or simply from bugs or hardware problems, but in all cases they can render the system unusable in the absence of proper protocols [1]. Research in distributed algorithms and Blockchain systems has led to a number of protocols for managing Byzantine behavior in a classical, permissioned, setting [2, 3, 4, 5]. Yet operation in open permissionless settings remains challenging [6]. Currently, used methods like Proof-of-Work (PoW) or Proof-of-Stake (PoS) each have their own limitations. PoW suffers from

enormous energy consumption, while PoS relies on the presence of a cryptocurrency or other similar asset.

Recent research has shown that, albeit promoted in the context of Bitcoin, the blockchain data structure is unnecessary to implement a cryptocurrency [7]. This has led to the appearance of a variety of proposals that implement cryptocurrencies with lighter primitives such as Byzantine Reliable Broadcast [8, 9]. This simplification is likely to extend to a variety of other applications that currently fall under the Blockchain hype, including distributed storage.

The goal of this internship is to assess the potential of the IPFS decentralized storage framework (https://ipfs.tech/ (https://ipfs.tech/)) to host Sybil-protection [10, 11, 12] and Byzantine-tolerance mechanisms.

Workplan

The recruited intern will perform the following tasks:

1. Perform a technological and literature review of existing protection mechanisms in IPFS. This includes the realization of small POCs and experiments to exercise IPFS' in-built protection mechanisms, and to contrast them to the existing literature on BFT and Blockchain algoritms.
2. In a second stage, the intern will explore how broadcast-based ledger-operations can be added to IPFS to improve mutability and resilience to BFT attacks. The goal is to produce an early prototype of such a capability, and, it time permits, start characterizing its performance (latency, scalability) and robustness.

Candidate profile

The recruited intern should be studying in his or her final year of Engineering (École d'ingénieur) of Master Degree (M2) in Computer Science or equivalent, with a strong algorithmic and systems background, in particular regarding large distributed computer systems. Good programming skills, and a willingness to learn about new techniques (such as Byzantine-tolerant algorithms and techniques) are also key, as well as good writing skills, and the ability to propose, present, and discuss new ideas in a collaborative setting.

Pay and benefits

The intern will be hosted in the Hive offices in Cannes and paid by Hive.

- salary: 1500 Euro monthly gross + 50 euro monthly net allowance to cover remote-work related costs
- Remote work policy: Up to 3 days per week
- Ticket restaurant. The number depends on the number of working days per month. The amount is 9.5 euro per ticket (3.80 euro paid by the employee and the 5.70 paid by Hive).

How to apply

Please send an email with your resume to hr@hivenet.com (mailto:hr@hivenet.com)

References:

- [1] L. Lamport, R. Shostak, and M. Pease. "The Byzantine Generals Problem". In: ACM

TOPLAS (1982). doi: 10.1145/357172.357176.

- [2] G. Bracha. “Asynchronous Byzantine Agreement Protocols”. In: Information and Computation 75.2 (1987), pp. 130–143. issn: 0890-5401. doi: 10.1016/0890-5401(87)90054-X.
- [3] D. Imbs and M. Raynal. “ Trading off t-Resilience for Efficiency in Asynchronous Byzantine Reliable Broadcast”. In: Parallel Processing Letters 26.04 (2016). doi: 10.1142/S0129626416500171.
- [4] A. Mostéfaoui, H. Moumen, and M. Raynal. “Signature-Free Asynchronous Binary Byzantine Consensus with t < n/3, O(n2) Messages, and O(1) Expected Time”. In: Journal of the ACM 62 (4 Aug. 2015). doi: 10.1145/2785953.
- [5] M. O. Rabin. “Randomized Byzantine Generals”. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. Los Alamitos, CA, USA: IEEE Computer Society, Nov. 1983, pp. 403–409. doi: 10.1109/SFCS.1983.48.
- [6] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovič, and D.-A. Seredinschi. “Scalable Byzantine Reliable Broadcast”. In: 33rd International Symposium on Distributed Computing, DISC 2019. Oct. 2019. doi: 10.4230/LIPIcs.DISC.2019.22.
- [7] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovič, and D.-A. Seredinschi. “The Consensus Number of a Cryptocurrency”. In: Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. ACM, 2019, pp. 307–316. doi: 10.1145/3293611.3331589.
- [8] A. Auvolat, D. Frey, M. Raynal, and F. Taïani. “Money Transfer Made Simple: a Specification, a Generic Algorithm and its Proof”. In: Bulletin of EATCS 132 (2020). hal: hal-02861511v3.
- [9] M. Baudet, G. Danezis, and A. Sonnino. “FastPay: High-Performance Byzantine Fault Tolerant Settlement”. In: 2nd ACM Conference on Advances in Financial Technologies. ACM, 2020, pp. 163–177. doi: 10.1145/3419614.3423249.
- [10] A. Bouchra Pilet, D. Frey, and F. Taïani. “Foiling Sybils with HAPS in Permissionless Systems: An Address-based Peer Sampling Service”. In: IEEE Symposium on Computers and Communications. IEEE, 2020. doi: 10.1109/ISCC50000.2020.9219606.
- [11] J. R. Douceur. “The Sybil Attack”. In: International Workshop on Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002, pp. 251–260. doi: 10.1007/3-540-45748-8_24.
- [12] G. Urdaneta, G. Pierre, and M. V. Steen. “A Survey of DHT Security Techniques”. In: ACM Computing Surveys 43.2 (Feb. 2011). issn: 0360-0300. doi: 10.1145/1883612.1883615.