Byzantine Tolerant CRDTs

Keywords

CRDTs, Byzantine Fault Tolerance

Context

An important challenge in P2P storage lies in the need to control the access to resources without relying on any central authority. A possible solution to this need lies in the use of Self-Sovereign Identity systems (SSI). An SSI makes it possible to assign users credentials and verify them in completely decentralized manner, without a trusted third party. However, existing SSI implementations rely on system-wide synchronization, generally implemented through the use of blockchain solutions.

Our intuition suggests that neither SSIs nor access-control systems require a blockchain. Rather, both only require strong coordination at a relativerly small scale and for specific tasks, while most operations can be implemented with low levels of coordination and consistency such as those provided by CRDTs (Conflict-Replicated Data Types) [1, 2]. Unfortunately, existing CRDTs cannot, apart from a few exceptions [3], withstand attacks or malicious behaviors, and it is not clear to what extent they can support access-control systems [4].

Goal of the Internship

This internship aims to explore the staate of the art of existing CRTDs, and design novel design Byzantine tolerant CRDTs that can support scalable decentralised access-control systems.

Main Tasks

- The intern will start by performing a thorough state of the art covering the topics of access control systems, CRDTs and byzantine fault tolerance.
- He or she will then identify the limtations of current CRDTs and specify the requirements for CRDTs or CRDT-like objects that can support p2p access-control.

- He or she will implement a prototype or a simulator, and/or work on a theoretical analysis of the proposed solution.

Logistics

This internship results from a collaboration between the WIDE team in Rennes (Davide Frey), the COAST team in Nancy (Claudia-Lavinia Ignat) and the Hive Company (Amine Ismail) located in Cannes (06).

The internship will take place in HIVE's headquarters in Cannes (06) and will be remunerated at a salary of E 1,329.05 (SMIC).

Desired Skills

- Basic knowledge of distributed algorithms
- Prior knowlege of CRDTs is not required but appreciated
- ability to move to Cannes for the duration of the internship

References:

[1] M. Shapiro, N. M. Preguiça, C. Baquero, and M. Zawirski. “Conflict-Free Replicated Data Types”. In: 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS 2011. Oct. 2011, pp. 386–400. doi: 10.1007/978-3-642-24550-3_29.

[2] L. André, S. Martin, G. Oster, and C.-L. Ignat. “Supporting adaptable granularity of changes for massive-scale collaborative editing”. In: Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2013). Austin, Texas, USA, Oct. 2013 [3] M. Kleppmann. “Making CRDTs Byzantine Fault Tolerant”. In: Proceedings of the 9th Workshop on Principles and Practice of Consistency for Distributed Data. PaPoC ’22. Rennes, France: Association for Computing Machinery, 2022, pp. 8–15. isbn: 9781450392563. doi: 10.1145/ 3517209.3524042.

[4] P.-A. Rault, C.-L. Ignat, and O. Perrin. “ Distributed Access Control for Collaborative Applications using CRDTs”. In: Proceedings of 9th Workshop on Principles and Practice of Consistency for Distributed Data. Rennes, France, Apr. 2022.