Postdoctoral position opening: security and performance improvement of distributed ledgers based on directed acyclic graphs.

Working environment

The successful candidate will join the Maths&Net research group, part of the Cybersecurity and Networking working group within the LabSTICC laboratory, located at IMT Atlantique, Brest, France. The opening is for 2 years.

Project’s summary

Distributed ledgers constitute one of the latest innovations in the distributed system field. They are mainly known through blockchain technology and Bitcoin cryptocurrency. A distributed ledger is a database distributed through the nodes of a peer to peer network, it is immutable and replicated on each node. They offer improved data transparency and integrity with respect to a centralized database.

A new type of DL, featuring better performance than blockchain based DLs — in terms of rate and transactions cost — has been introduced by IOTA Research Foundation[4]. Such DL is based on an underlying structure given by an acyclic directed graph, where each new transaction has to validate two previous ones in order to get attached to the DL. Such structured is the so called Tangle.

The Tangle promises to be a DL well suited for several different use cases, such as personal identification data bases, or the industry 4.0. It is thus of paramount importance to guarantee the robustness and security of such a register [0].

Several questions arise regarding the functioning and efficiency of this new technology, for instance:

- Register’s performance: under which conditions is the system stable? (regarding the number of unvalidated transactions) To which extent, network’s delay or other input parameters, such as the number of transactions sent by each node over a unit of time, have an impact on the performance of the register? Which are incentives and which are obstacles making nodes participate or not in tasks related to the maintenance of the register (transactions’ validation, protocol violations).
- Security of the protocol: which are the register vulnerabilities and which countermeasures to them exist? How many nodes are to be corrupted in order to modify some portion of the register?

In particular, we are interested in aspects regarding performance and security of such registers. In this sens, our objective is to propose access control mechanisms, making it possible to prevent spam and related attacks (such as denial of service) while optimizing the functioning of the register. Moreover, these algorithms must guarantee a fair resource sharing among participating nodes while being robust to the presence of byzantine nodes (i.e. not following the defined protocols).

We propose a twofold approach, namely theoretical and practical, aiming to compare theoretical results with ground truth. On the one hand, we aim to mathematically model the distributed system and propose safe algorithms, while optimizing system’s performance. On the other hand, we are interested in implementation aspects and validation of theoretical proposals through the implementation over our running testbed.
The project is structured around three general objectives (GO), namely: -GO1 Stochastic modeling of DAG-based distributed ledgers, aiming to understand the possible attacks blocking the validation of legitimate transactions. We aim also to deduce pertinent performance metrics, such as the expected validation time of a transaction. -GO2 Distributed algorithms improving system’s performance and featuring robustness properties against attacks, and against protocol deviations, and,-GO3 Model and algorithm implementation on a testbed.

Different solutions for access control in DAG-based DLs exist in the literature. [1] proposes a mechanism which is based on a proof of work, without taking into account nether network’s performance nor node’s utilities nor the existence of malicious nodes. Recently, [2] has proposed a congestion control algorithm based on nodes’ reputations and robust to the presence of malicious nodes, but results’ validation is numerical rather than analytical. Moreover, how reputation -a key value of the model- is computed is not addressed in the paper. Within out research group, we have implemented a Tangle’s testbed, which allowed us to obtain performance data and to test our first propositions. The results of such work has been published in [3], where an access control algorithm, optimizing nodes’ utilities and network performance, is proposed.

We have also addressed a theoretical study about stochastic modeling of the Tangle, subject of a recent research internship within our research team. A scientific publication, result of this work, is now under submission.

To the best of our knowledge, control access solutions, which take into account the stochastic nature of the system, the network’s performance and robust to attacks, have not yet been proposed in the literature.

**Expected outcomes**

From a theoretical point of view, the two main expected outcomes of the project are: (1) a model allowing to evaluate the performance of DAG-based DLs and the impact on the register’s state of deviations in the behavior of nodes. (2) proposal of new admission control algorithms under the presence of byzantine nodes. These results might provide new insights in the field of DLs but also in the field of federated machine learning, new discipline focusing on machine learning in distributed environments in a secure way (not sharing data).

**Candidates profile**

The successful candidate would ideally fulfill the most of the following requirements:

- Solid mathematical background
- Some experience or knowledge in networking and network security
- Some computer science skills, allowing the candidate to create and manipulate simulation scripts, to develop working code, to manipulate collaborative environments, as for instance knowledge of programming languages such as Python, bash, Go and changes tracking systems such as git.
- Good communication skills, excellent written English skills.
- Motivated, inquisitive and self-driven

The project is partially founded by Brittany region, which adds an extra requirement for candidates: eligible candidates must have spent at least 18 months outside France during the period spanned between May the 1st 2019 and the project’s kick-off.


