nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Nomadic Labs Internships

Nomadic Labs houses a R&D team of more than 50 engineers, most of them PhDs, who apply their expertise in **distributed**, **decentralized** and **formally verified** software.

Joining one of our teams as an intern, you will grow your skills working with talented engineers, mixing industrial and academic skills in a collegiate and collaborative work culture to build a free and open-source decentralized ecosystem that is dedicated to social good as well as technical excellence.

Nomadic Labs helps to build **Tezos**, the self-amendable, eco-friendly blockchain, and associated tools and software, applying computer science research to real-world industrial contexts:

- We build and distribute Octez, an OCaml implementation of the Tezos protocol.
- We participate in amendments to upgrade the Tezos economic protocol.
- We develop innovative solutions to improve privacy using cryptographic tools.
- We develop state-of-the-art consensus algorithms (such as Emmy* and Tenderbake) that will be at the heart of future decentralized software.
- We develop Umami, a ReasonML-based innovative Tezos Wallet building on our expertise of the core Tezos protocol.
- We develop verification frameworks and tools to prove the correctness of OCaml programs, which our developers apply to assure the quality of our industry-scale code, and specifically Octez.
- We develop verification tools and frameworks for smart contracts and apply them to ensure their safety.

All our code and tooling is made available on open-source licenses, for the benefit of the wider programming community.

This catalog presents our current internship proposals and topics you may want to propose to tackle with us in projects of your own

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Internships at Nomadic Labs

Nomadic Labs houses a team focused on Research and Development. Our core competencies are in programming language theory and practice, distributed systems, and formal verification. Our strength lies in a unique mix of skills and experience, allowing us to transfer the best of academic research into real world applications.

We contribute to the development of software at the core of the Tezos blockchain – including its *smart-contract* language, Michelson – to produce state-of-the-art formal verification tools for *smart contracts* and to apply formal methods on as many software components as possible to improve our products.

Internship topics

- Cartography, monitoring and analysis of the p2p network
- Ad-hoc Static Analysis of Octez
- Memory footprint analysis of Ocaml concurrent programs
- FAT CAT: Formal Acceptance Testing of Contracts for Administering Tokens
- Generation of Scenario Tests
- MechaTez: Formally Verifying Critical Features of Tezos Protocols
- Live Monitoring of Tezos Nodes : Tezos-metrics
- Integrating static analysis in smart-contract development tools
- How to Reason on Traces between Tezos Nodes
- Contribute to the next Tezos blockchain protocol amendment
- React/Reason programming on a wallet application in a blockchain setting
- Improve our Formal Verification Framework
- Comparing Program Proof Tools for OCaml Programs in an Industrial Setting
- Propose your own subject

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Cartography, monitoring and analysis of the p2p network

Tutors : Vivien Pelletier, Julien Tesson, Ilias Garnier, Mathias Bourgoin

A blockchain is a decentralized system implementing a consensus algorithm over a peer-to-peer (p2p) network.

The consensus algorithm implemented in Tezos is robust against partial failures of the underlying p2p network. However, a healthy network ensures a faster diffusion of messages and reduces the likelihood of temporary divergences caused by nodes having a partial view of the network.

Quantifying healthiness of the p2p layer requires an understanding of its key properties, such as its *shape*, its *size*, and the laws governing its evolution. Even though the decentralized nature of the network and its high dynamicity make it practically unfeasible to map it exhaustively, some useful properties can be inferred from partial information provided by dedicated "cartographer" nodes, such as observations of the structure of their neighborhood and of temporal shifts in the reception of messages.

Goals

The goal of this internship is to develop mathematical and software analyses for the peer-to-peer network of the Tezos blockchain, as follows:

1. Building upon existing work, you will build a cartographer node to estimate simple metrics, such as the size of the network, its diameter, or the lifetime of adjacent nodes.
2. You will refine these results by deploying a sub-network of cartographer nodes and developing tools able to aggregate the data that it gathers.
3. You will design and implement a statistical model to infer properties of the network topology from the aggregated data gathered by the cartographer nodes.

Requirements

You should have a good knowledge of the OCaml programming language and be eager to explore the literature pertaining to the statistical estimation of structural properties of graphs.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Ad-hoc Static Analysis of Octez

Tutors : Thomas Letan and Mehdi Bouaziz

One of the distinguishing feature of Tezos is its self-amendment property. Every now and then, the Tezos ecosystem is asked through a vote procedure to decide how the chain will evolve. What that means in practice is that software updates (called *protocols* in Tezos) are regularly proposed, elected, and finally automatically deployed. In practice, a new protocol is deployed every three or four months.

The downside of this approach is that deploying a protocol takes time, and is not suited to deal with the discovery of critical bugs *after* said protocol has been deployed. Furthermore, the Tezos blockchain is used to manage sensitive, valuable assets that a bug could jeopardize.

As a consequence, it is essential to ensure the quality of a protocol prior to proposing it to the ecosystem. One possible approach to is to rely on automated tools, such as static analyzers, to improve the quality of the codebase. During the Summer of 2021, we sent a survey to the programmers involved in the development of Octez to tell us which properties they would like to see checked automatically. Unfortunately, it appears that there is not yet a silver bullet tool capable of addressing our needs.

Internships goals

The goal of this internship is to bootstrap the effort to provide ad-hoc, relevant static analyses for the Octez codebase. Based on the result of our 2021 survey mentioned above, the intern will conduct the necessary software development to implement the most-wanted analyses (*e.g.*, metrics such as functions size or documentation coverage to measure code quality, call graph analyses to detect unwanted side effects, etc.).

This could mean extending an existing analyzer, but it could also mean initiating the development of a new tool.

In either case, the goal of the internship is to be able to provide a pragmatic tool that can be integrated into a development workflow. Even if the primary objective of the internship is to target Tezos workflow, the tool should be generic enough so that it can contribute to the OCaml ecosystem in the long run. To this end, the resulting tool should be published under the terms of the MIT license.

Requirements

The successful applicant should have a good knowledge of the OCaml programming language. A knowledge in the tools used by developers to collaborate to develop Octez would be a nice bonus. This includes `git`, Gitlab CI, `dune`, and `opam` among others.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Memory footprint analysis of Ocaml concurrent programs

Tutor : François Thiré

The Octez suite of Tezos blockchain-related software, developed by Nomadic Labs and others, is a highly complex software artefact: the codebase is relatively large, it is highly concurrent, and it is designed to be resilient to attacks from malicious peers. Finding errors in such large piece of software can be very difficult and in particular, *memory leaks* are notoriously difficult to track. This is because memory-allocation in inherently hard to analyse:

1. Memory-allocation is implicit, and the lifetime of an allocated object is non-deterministic because of how the incremental, generational, OCaml garbage collector works.
2. Concurrency in the code makes usual memory analysis tools (such as statmem-prof, valgrind or landmarks) unusable
3. Memory leaks can come from a so-called *allocation race*, meaning that the program allocates memory faster than the garbage collector can deallocate it – so that even though every memory cell that is allocated will eventually get deallocated, in practice the stack of pending deallocations grows without bound.

Internship goals

The goal of this internship is to develop tools and/or libraries to help developers find memory-related bugs. The intern will choose amongst the proposed topics as follows:

Make OCaml's values traceable: a library to analyze and trace the lifetime of OCaml's values and generating a readable report.

Memory footprint with `Lwt`: Octez concurrency is obtained thanks to the `Lwt`[1] library for cooperative threading. To analyse clearly the memory of a program, one needs to separate the `Lwt` specific part from the `Lwt` agnostic part.

Profiling `Lwt` overhead: In addition to the inner code of Octez, `Lwt` is used by its external dependencies, therefore it is hard to predict and observe which "threads" are created at runtime. Profiling `Lwt` would help gain a better understanding of the different "threads" which are running/created by a program, and to identify hot spots.

Eliminate `Lwt` interference from profiling: To benchmark and understand a program's allocation behavior, we would like to isolate `Lwt` from the traces of memory analysis. This could be implemented on top of the `memtrace`[2] library for example.

Requirements

The intern should have a good knowledge of the OCaml programming language and have an appetite to delve into the inner workings of the OCaml compiler. Some knowledge of C or assembly language would also be useful.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] https://ocsigen.org/lwt/latest/manual/manual
[2] https://github.com/janestreet/memtrace

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

FAT CAT: Formal Acceptance Testing of Contracts for Administering Tokens

Tutors: Arvid Jakobsson, Kristina Sojakova

Blockchains, such as Tezos, implement **tokens**: cryptographically secured assets representing the ownership of a value. Chains typically have one **native** token (in the case of Tezos; the **tez**), but also allow developers to create additional tokens for other types of value. In Tezos, this is done by writing a **smart contract**: a small piece of software deployed on-chain. The smart contract defines how tokens are created, removed and transferred between users.

Interoperability of token contracts is important: they form key components in larger systems of inter-acting smart contracts. The FA1.2 standard have been proposed as a common interface all token contracts should expose. In addition, security of token contracts is clearly paramount: we wouldn't want any tokens to get lost or stolen. For these reasons, Nomadic Labs have formalized the FA1.2 standard using Mi-Cho-Coq, a smart-contract verification platform for Tezos. Using it, we have ensured standard compliance of several popular FA1.2 implementations, and increased our confidence in their security.

Goals of the internship

Currently, a correctness proof must be hand-written to verify compliance with the formalized standard. This is time consuming and requires Coq expertise beyond the average smart contract developer. The first step of this internship is to use the FA1.2 formalization as base for implementing a compliance testing suite in Coq. The intern should prove in Coq, using the standard's formalization, that *each compliant token contract must pass the verification of the test suite*. In other words: prove that the compliance suite itself is coherent with respect to the standard.

In the second step, the intern will make the conformity-testing tool available through an online interface. Smart contract developers will be able to test the compliance of their smart contract from the comfort of their browser, without having to install Coq or write any proofs.

Requirements

Requirements are (in decreasing order of importance):

- Familiarity with functional programming, e.g. OCaml, Haskell or Scala.
- Experience with the Coq proof assistant.
- Familiarity with the extraction mechanism of Coq is a plus.
- Having some elementary notions of web programming is a plus.

Further reading

- FA1.2: Approvable Ledger Interface
- FA1.2 Approvable Ledger, formal verification by Nomadic Labs
- Formal Verification of ERC20 Contracts
- ERC20 Token Verifier

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Generation of Scenario Tests

Tutors: Zaynah Dargaye, Arvid Jakobsson

Tezos is a blockchain developed with a focus on governance and security. It is highly safety-critical software and so requires a high level of code quality.

To this end, the Tezos code-base is entirely written in OCaml, a strongly typed functional language. In addition, Nomadic Labs applies **formal verification** and **testing**. In terms of testing, we use unit, integration and property-based tests. Currently, we push for a wider application of property-based tests. Taking this further, we are working on automatic generation of the property-based tests themselves. Generation enables particularly efficient validation of code: it automates boilerplate tasks (saving time and avoiding bugs) and thus lowers the expertise needed to develop tests.

Use-case tests correspond to use-case scenarios. A use-case scenario describes the behavior of an applied functionality under a characterized set of parameters. For a given functionality, the set of use-case scenarios describes all its possible behaviors. A use-case scenario is validated by a series of tests on every called function.

Goal

Goals are in order:

1. To create a tool for specifying use-case scenarios of OCaml functions in an API, similar to tags in ocamldoc comments[1].
2. To implement a PPX[2] code generator that transforms annotations into scenario tests.
3. To create a tool that generates a report for all use-case scenarios of a functionality.

Requirements

Requirements are:

1. Knowledge of OCaml programming.
2. Basic understanding of formal verification and testing.
3. Experience of a version control system (like git) is a plus.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] OcamlDoc syntax: https://caml.inria.fr/pub/docs/manual-ocaml/ocamldoc.html#ss:ocamldoc-syntax

[2] PPX manual: https://ppxlib.readthedocs.io/en/latest/ppx-for-plugin-authors.html

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

MechaTez: Formally Verifying Critical Features of Tezos Protocols

Tutors : Thomas Letan and Yann Régis-Gianas

One of the distinguishing feature of Tezos is its self-amendment property. Every now and then, the Tezos ecosystem is asked through a vote procedure to decide how the chain will evolve. What that means in practice is that software updates (called *protocols* in Tezos) are regularly proposed, elected, and finally automatically deployed. In practice, a new protocol is deployed every three or four months.

The downside of this approach is that deploying a protocol takes time, and is not suited to deal with the discovery of critical bugs *after* said protocol has been deployed. Furthermore, the Tezos blockchain is used to manage sensitive, valuable assets that a bug could jeopardize.

As a consequence, it is essential to ensure the quality of a protocol prior to proposing it to the ecosystem. One possible approach to is to rely on formal methods to formally verify the correctness of (critical part of) a protocol. Because Tezos protocols are developed in OCaml, the Verification team of Nomadic Labs is exploring the use of FreeSpec to tackle this challenge. FreeSpec is a reasoning framework for the Coq theorem prover. The resulting project is called MechaTez.

Internships goals

The goal of this internship is to take part in the MechaTez project. More precisely, the intern will leverage MechaTez to formally verify one feature of Tezos, either one that is already integrated into the codebase or one that is still in development. This implies:

- understanding the OCaml implementation of said feature,
- porting this implementation in Coq,
- formalizing both the properties of the feature and the hypotheses it relies on,
- proving the correctness of the Coq model wrt. these properties,
- validating of the Coq model against the original implementation.

We are interested in proving functional correctness (wrt. a formal specification) and security properties (*e.g.*, storage integrity, secret confidentiality, resistance against cache poisoning, etc.).

Because MechaTez is still in a early stage, the intern will be encouraged to contribute to the ecosystem supporting MechaTez, notably FreeSpec (the reasoning framework) and `coqffi` (a tool used in MechaTez to generate Coq FFI modules for the OCaml protocol implementation).

Requirements

The successful applicant should have a good knowledge of the OCaml programing language. They should be familiar with at least one theorem prover, more preferably Coq. Finally, they should be familiar with Hoare Logic, and formal verification of software programs.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Live Monitoring of Tezos Nodes : Tezos-metrics

Tutors : Pietro Abate

Tezos-metrics is an OpenMetrics-compliant server which uses the Octez libraries (the Tezos node implementation from Nomadic Labs) to scrape data from a Tezos node and feed this information to time series databases such as Prometheus,

The Tezos-metrics project is nearly two years old and has been in internal use at Nomadic Labs for development and testing of live code.

The project aims to release a free and open-source Tezos-metrics precompiled binary, and corresponding self-contained docker image, for use by Octez developers and the wider community to monitor node statistics, conveniently and in real time.

1. The first release will support key shell metrics and offer limited support for protocol metrics.
2. A second release will add bakers and additional protocol metrics.
3. A third phase will provide Tezos-metrics as an opam library for Octez with a well defined api, and so allow a node to serve open-metrics directly without an external scraper, lowering the load on the RPC interface.

Providing metrics about the inner working of the node, the p2p layer and the protocol (and henceforth the Tezos network), can help developers to diagnose problems, collect historical data, and monitor network health.

Since Tezos-metrics is integrated in the Octez code base, this binary can evolve together with the Octez suite, never getting out of sync. This is accomplished by directly using the Octez data-encodings definitions. Tezos-metrics also has a system to change protocols, making it a valuable tool to diagnose issues and gather simulated data regarding protocol updates.

Internships goals

The intern will enhance and test Tezos-metrics: You will learn low-level details of the Octez codebase and the Tezos protocol, and focus on the development of protocol metrics via a plugin system designed to allow Tezos-metrics to evolve alongside with the Tezos protocol.

Part of the work will also concern the development of a solid test framework for Tezos-metrics.

Requirements

Since Tezos-metrics is written in OCaml, you should be proficient in OCaml programming, and in particular you should have some familiarity with Lwt, the *lightweight threads* OCaml library.

An understanding of the OpenMetrics standard and of Prometheus/Grafana is also a plus.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Integrating static analysis in smart-contract development tools

Tutors: Alexandre Doussot, Guillaume Bau, Mehdi Bouaziz

A smart contract is a distributed application that is deployed on a blockchain to administer rules and automate tasks. Thus: smart contracts are how blockchains are made programmable.

Unfortunately, a smart contract may be impossible – or at least very inconvenient – to change once it is deployed. Errors in smart contracts have led to the theft or blockage of the tokens they administer, often representing large amounts of value (e.g. as money or important certificates).

As such, the correctness and security of smart contracts is critical, both to the users of specific smart contracts ("Do I trust this smart contract with my money?"), and to the viability and value of blockchain platforms overall ("Do smart contracts on this blockchain have a good reputation?").

Several projects focuses on helping dApps developers improve the code quality and security of their smart-contracts written in Michelson, Tezos' smart-contract language, by means of static analysis: - CIAOPP - Tezla - Mopsa - Helmholtz

On the other hand, dApps developers often use higher-level, more developer-friendly languages, such as Ligo, Smartpy, Morley, Archetype, that are compiled to Michelson.

Goals of the internship

This internship aims to make state-of-the-art static analysis tools for Michelson more accessible to Tezos dApps developers by integrating them into the Tezos development environment, both for programming directly in Michelson and *also* for users of higher-level languages.

Specifically the intern will:

- define a generic interface to have results of static analysis shown in Michelson development tools, probably based on LSP or SARIF;
- extend this interface to translate results on Michelson to results on higher-level languages, in collaboration with developers of these languages; and
- pick a static analysis tool and a development tool, implement this integration, and collect feedback on how to improve it.

A stretch goal will be to set up a static-analysis-as-a-service server to allow developers to benefit from these tools online and without a local install.

Requirements

Interest in helping developers build secure software, knowledge in OCaml and Javascript are required.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

How to Reason on Traces between Tezos Nodes

Tutors: Zaynah Dargaye, Paul Laforgue, Julien Tesson

We devote a lot of resources towards the quality of the implementation of the Tezos blockchain. Formal verification is a natural part of this effort, helping to ensure that the code behaves as predicted.

The challenge is to reconcile this quality requirement with the imperatives of software that is in perpetual evolution – all the more so because verifying blockchain software in particular means understanding and being able to reason about a distributed system in an open and potentially hostile environment.

We are building a suite of formal tools designed to provide strong formal guarantees of correctness while integrating smoothly into the Tezos blockchain development workflow.

Our suite for formal verification includes a high-level specification of a Tezos network that asserts global invariants to be preserved by each node. From these global invariants, we derive the properties that each node's component has to satisfy. The Tezos blockchain is a message-passing protocol. Its correctness verification requires reasoning on message traces. By formalizing the Tezos protocol as a set of "correct" messages traces, we can derive: 1. a formal specification against which to verify the OCaml implementation (e.g. "This implementation only produces correct traces"), and 2. a monitoring tool to detect incorrect traces in the network. Finally, reasoning on the message contents enables reasoning on global properties. In Asphalion[1] for example, the reasoning takes place in a distributed lift thanks to a knowledge logic.

Goal

The goal of the internship is to design and develop a logical framework to reason on message traces exchanged during a message-passing protocol.

The successful applicant will be in charge of: - gathering the state-of-the-art of formal reasoning on message traces, - designing and implementing a well-formed checker, - designing and implementing a logical framework to reason on traces.

Requirements

- *Essential:* A good grasp of formal methods and program specification.
- *Helpful:* Knowledge of distributed systems.
- *Nice to have:* Experience of version control tools (e.g. git).

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] https://vrahli.github.io/articles/asphalion-long.pdf

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Contribute to the next Tezos blockchain protocol amendment

Tutors : Mehdi Bouaziz

One of the distinguishing feature of the Tezos blockchain is its self-amendment property. Every now and then, the Tezos ecosystem is asked through a voting procedure to decide how the chain will evolve. What that means in practice is that software updates (called *protocols* in Tezos) are regularly proposed to the community, voted on, and finally automatically deployed. A new protocol is deployed every three or four months.

Internships goals

The intern will participate in the development of a new feature to be integrated into a forthcoming protocol amendment, from start to finish: from the feature's initial design, through to seeing the final software integrated into Tezos, deployed globally to the live blockchain, and used by members of the Tezos ecosystem.

Specifically, the development process involves:

- choosing a feature to implement;
- designing, specifying;
- implementing the feature, testing, debugging;
- shepherding the integration of the feature in the amendment;
- communicating about the feature.

The specific feature will be decided at the beginning of the internship, based on intern's interests and with input from the community. Examples of features include: a new kind of blockchain operation; additions to Tezos' smart contract language Michelson; changes in the consensus algorithm; and new economic incentives or adjustments to existing incentives.

All of these steps include key aspects of industrial software engineering, including: *communication and collaboration* (with the community, the testing and verification teams, and the protocol development teams); *collaborative software development* (version control, code review); and highly rigorous *quality- and security-assurance* of the code (different levels of testing, verification, development-aiding tools).

Requirements

The successful applicant should have a good knowledge of the OCaml programing language and a vigorous interest in security and code quality.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

nomadic labs

Paris, France
https://www.nomadic-labs.com
internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

React/Reason programming on a wallet application in a blockchain setting

Tutors : Rémy El Sibaïe, Pierrick Couderc

The Tezos Blockchain[1] is a decentralized system, relying on a peer-to-peer network, and whose consensus algorithm is based on a proof of stake protocol

Tezos introduces the *tez* token on the economic layer and features smart-contracts written in the Michelson language[2]. Storing and exchanging *tez*, as usually done in the crypto-currency world, use exchanges and client wallet applications with software or hardware secured storage.

Umami[3] is a wallet developed at Nomadic Labs, the main contributor of the reference implementation of Tezos named Octez. Umami is designed to handle the main operations of a Tezos client (including *transfer* and *delegation*), to manage local accounts securely, and to permit interaction with community APIs and with smart contracts.

Internships goals

The goal of this internship is to introduce the intern into a development team for for client-servers based application interacting with a blockchain network, and in particular for Umami.

The intern will have to use several concepts and technologies:

- ReasonML[4]: a functional programming language with a strong, static type system
- React: a popular framework for Web-client programming with reactive systems
- Client-server+blockchain architecture: some constraints are unique to decentralized networks and have a huge impact on this kind of application
- Software engineering good practices: advanced git usage, writing clean merge requests, code peer-reviewing

Proficiency in these technologies is not required. If necessary, the intern will start learning technologies by developing simple tasks, and then be introduced to a wider subject on which they will have more autonomy.

Requirements

The intern should know about functional programming and have experience, through studies or internship, with at least one language of this category (OCaml, Reason, Haskell, Scala, Closure, etc.). The intern should have experience, through studies or internship, with at least one of web client programming or mobile applications programming, *e.g.*, Javascript frameworks (react, angular, etc), Android/iOS, others. The intern should be able to take initiatives and be as independent as possible to solve the different problems faced. They should value code quality, listening carefully to given instructions and a good ability to learn.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] https://tezos.com/learn/what-is-tezos/
[2] https://tezos.gitlab.io/active/michelson.html
[3] https://umamiwallet.com/
[4] https://rescript-lang.org/

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Improve our Formal Verification Framework

Tutors: Zaynah Dargaye, Thomas Letan, Boubacar Sall.

The Tezos blockchain places a premium on the quality of its implementation. Formal verification is a natural way to ensure that the code behaves as predicted.

The challenge is to meet both this quality requirement and the reality of software in perpetual evolution. Moreover, verifying a blockchain means understanding and being able to reason about a distributed system in an open and potentially hostile environment.

We are building a suite of formal tools to take advantage of the strongest formal guarantees while adapting to the Tezos blockchain development process.

These efforts include:

- Formal specification: component specification designs with proof in mind.
- Proof of correctness of the entire code base: it implements a blockchain.
- Code correction: each component of the code behaves as expected.
- Extending and improving the tools used.

Our tools of choice are Coq, FreeSpec[1], and property-based testing.

Goal

If you want to participate in these efforts, either through its implementation on one of our critical components or if you want to participate in the design and implementation of formal tools in an industrial setting, we have a set of topics to offer.

The successful applicant will be in charge of:

1. Documenting the pertinent state-of-the-art for the topic.
2. Describing, in a rigorous manner, the methodologies and tools that she(he) wants to explore.
3. Implementing them on a realistic use case.

Requirements

To tackle this subject, training in formal methods and program specification is essential. Familiarity with a formal verification tool is welcome, and experience with Coq is a definite plus. Experience with source management such as git is welcome.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] https://hal.inria.fr/hal-02422273

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Comparing Program Proof Tools for OCaml Programs in an Industrial Setting

Tutors: Zaynah Dargaye, Thomas Letan.

The Tezos blockchain places a premium on the quality of its implementation. Formal verification is a natural part of this to ensure that the code behaves as predicted.

The challenge is to meet both this quality requirement and the reality of software in perpetual evolution. Moreover, verifying a blockchain means understanding and being able to reason about a distributed system in an open and potentially hostile environment.

We are building a suite of formal tools to take advantage of the strongest formal guarantees while adapting to the Tezos blockchain development process.

Our suite of tools for formal verification includes a framework for deductive verification in Coq, FreeSpec[1]. Our choice was motivated by our expertise as proof engineers according to the following criteria: coverage of our codebase, the high degree of formal guarantees provided, compatibility with high-level reasoning, usability, maintainability of the tool, and the proof scripts.

We would like to challenge this choice to other existing solutions for program verification through a feedback and comparison document on our criteria.

Goal

The goal of this internship is to drive a comparison between FreeSpec and other program proof tools for OCaml by experimentations. The witness of thoses experimentation will be a component that is already verified in our framework. The program proof part will be run in the alternative tools. A report on the experimentation will focus on our criteria and provide a comparison and recommendation for improvement.

The successful applicant will be in charge to:

- select two other program proof tools based on their descriptions or accessible information,
- perform the verification in both alternatives
- Write clear feedback experiences

Requirements

For this, a background in formal methods and program specifications is essential. Familiarity with a formal verification tool is welcome. Practical experience developing in OCaml is a definite plus. Experience with source management such as git is welcome.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).

[1] https://hal.inria.fr/hal-02422273

nomadic labs

Paris, France

https://www.nomadic-labs.com

internship@nomadic-labs.com

Located in France in Paris, Nomadic Labs' expertise centers around the research and development of products and services in many domains of computer science, including distributed, decentralized, and formally verified systems.

Propose your own subject

You want to work at Nomadic Labs, but none of our internship topics really suit you? In that case, do not hesitate to reach to us. Mention which projects interest you the most, and depending on your profile, we will try to write an internship subject together. Here are some examples of topics that we might be interested in:

1. Participating in the implementation of Octez, the economic protocol and the Umami wallet by
   - improving the P2P, storage and other systems layers of Octez
   - engaging in the design and implementation of new features and improvements of the Tezos protocol using OCaml
   - joining the development of Umami, an Electron-based Wallet, developed using ReasonML and React and its indexer
2. Designing or contributing to development tools by
   - improving and extending our *monitoring and profiling tools* using OCaml and commonly used monitoring software and frameworks
   - improving our OCaml-focused *testing frameworks*
   - helping improve our *gitlab-based CI/CD processes*
   - improving our *release management processes*
   - improving our *development environments* for the core Tezos application and our Dapps
3. Participating in the verification efforts of Smart contracts and the Octez code-base by
   - designing component specifications with proof in mind using Coq and FreeSpec
   - designing component specifications and applying model checking to assert their correctness
   - participating in the proof of correctness of the entire Octez code base using Coq
   - ensuring each components behaves as expected via property based testing
   - contributing to Mi-Cho-Coq, our Smart Contracts verfication framework
   - using Mi-Cho-Coq to verify Smart Contracts properties
   - improving our tools and verification frameworks
4. Joining our research efforts on privacy and consensus algorithms by
   - implementing state-of-the-art cryptographic solutions into the Tezos protocol
   - participating in our efforts to integrate existing cryptographic libraries binding Rust and OCaml
   - evaluating, testing and comparing innovative consensus algorithm
   - participating in the implementation of the future consensus algorithms of the Tezos protocol
   - improving our consensus algorithms simulation and testing frameworks

Nomadic Labs is opened to talented students and will help you grow your technical and soft skills in a thriving environment.

Internship Context

You will work at the Nomadic Labs' offices in Paris.

Participating in a large scale open-source project you will have to rapidly learn to use collaborative tools (Git, *merge request*, *issues*, gitlab, continuous integration, documentation) and to communicate about your work. The final results might be presented at an international conference or workshop.

You will have a designated advisor at Nomadic Labs and will have to work independently and to propose thoroughly-considered solutions to the different problems you will have to solve. You will be encouraged to seek advice from members of the team.

Intellectual Property

All material produced (essays, documentation, code, etc.) will be released under an open source license (e.g. MIT or CC).