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. We believe our strength lies in a unique mix of skills and experience, allowing us to transfer the best of academic research into real world applications.

Our current main activity is to 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 within our products.

Internships topics

- Cartography, monitoring and analysis of the p2p network
- Bindings to multiple languages for Tezos
- Energetic profiling of Tezos
- Linear Types for secure data
- Bring Michelson Coq smart contract model to the web
- Michelson by Example
- Create OpenAPI based specification for Tezos
- Protocol testing environment
- Zero Knowledge Proof Scheme Implementation
- Zero Knowledge Proof for Off-Chain Computation

Internship Context

The intern will work at the Nomadic Labs' offices in Paris or Grenoble. Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Cartography, monitoring and analysis of the p2p network

Tutors: Julien Tesson, Ilias Garnier, Mathias Bourgoin

Blockchains are decentralized systems implementing a consensus algorithm on 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 the structure of their neighborhood and measures of temporal shifts in the reception of messages.

Internships goals

The goal of this internship is to develop mathematical and software analysis for the peer-to-peer network of the Tezos' blockchain. Building upon existing work, the intern will build a cartographer node, which will be able to estimate simple metrics, such as the size of the network, its diameter, or the lifetime of a node.

In order to further refine these results, the intern will deploy a sub-network of cartographer nodes and develop tools able to aggregate the data from this sub-network.

In a second step, the intern will design and implement a statistical model able to infer properties of the network topology from the aggregated data gathered by the cartographer nodes.

Requirements

The successful applicant 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

The intern will work at the Nomadic Labs' offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Blockchains are decentralized ledgers managed using a distributed peer-to-peer network. Tezos is a blockchain and a smart contract platform, which development focus on governance and security. The Tezos code-base is entirely written in OCaml which is a strongly typed functional language.

Currently, to build applications on top of the Tezos platform, developers are forced to rewrite basic building blocks to interface their applications with the underlying network. These user-level applications are often written using other programming languages, frequently tightly coupled with a specific platform (e.g. Swift and Kotlin).

**Internship goal**

This project aims to bridge the gap by making the Tezos code-base, in particular the client-side libraries, directly available to these foreign platforms, removing the need to re-implement basic functionality from scratch, and allowing developers to concentrate their effort on the user interface.

OCaml provides a powerful framework to build OCaml to C/C++ bindings in a semi-automated fashion: the Ctypes library. The project will involve the following steps:

- Complete, test and distribute an existing OCaml to C/C++ binding for Tezos
- Create an initial Proof of Concept by writing a basic Python binding leveraging the C/C++ Tezos interface
- Depending on the time, the completion of these subtasks is foreseen:
  - Design a complete Python binding; test and distribute
  - Design a complete Rust binding; test and distribute
  - Design a complete Kotlin binding; test and distribute
  - Design a complete Swift binding; test and distribute

**Challenges**

Apart from technical difficulties, possible challenges are:

- the design of a modern and usable library, adapted to each target language.
- distribution and testing of the Tezos library using state-of-the-art tools.
- compiling and testing the Tezos library on different hardware architecture and environments.
- learning how to use continuous integration tools and integrate this work into the Tezos code-base.

**Requirements**

The successful applicant should have a basic knowledge of the OCaml programming language and C/C++. Knowledge of Python, Kotlin/Android SDK, and/or Swift/OSX is a plus, but not essential.

**Internship Context**

The intern will work at the Nomadic Labs' offices in Paris or Grenoble. Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Energetic profiling of Tezos

Tutors: Victor Allombert, Mathias Bourgoin, Julien Tesson

Blockchains are decentralized ledgers managed using a distributed peer-to-peer network. Different entities can interact with/within this network: nodes that replicate the state of the ledger, validators that handle the validity of operations and aggregate them into blocks, etc. There can be a wide variety of different and rather specific entities on each blockchain. Most blockchain software can be executed on multiple hardware. Thus, the network can also be very heterogeneous in terms of hardware.

The energy footprint of each entity can also be very different. For instance, the high energy consumption of proof-of-work-based validators (e.g. Bitcoin miners) is well known and studied\(^1\). Proof-of-stake-based blockchain validation is very lightweight and consumes less energy than its proof-of-work counterpart.

**Internship goal**

The goal of this internship is to estimate the energy consumption of the proof-of-stake Tezos blockchain. Using modified nodes and validators, the intern will first profile the energy consumption of each entity in a controlled environment using different scenarios. Then, the intern will apply their measurements to the actual network, to estimate the actual consumption of the overall blockchain, comparing its result to existing (or new, if needed) measurements on other blockchains.

**Requirements**

The successful applicant should already be familiar with OCaml. A knowledge of hardware architecture would be a plus.

**Internship Context**

The intern will work at the Nomadic Labs' offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).

Linear Types for secure data

**Tutors : Pietro Abate, Julien Tesson**

Blockchains are decentralized ledgers managed using a distributed peer-to-peer network. Tezos is a blockchain and a smart contract platform developed with a focus on governance and security. The Tezos code-base is entirely written in OCaml which is a strongly typed functional language.

The client part interacting with the Tezos blockchain, so-called digital wallets, is the software component (sometimes coupled with a hardware secure storage) entrusted with managing the private keys and identities of each user.

Linear types give guarantees that a value can only be used once. They can be used to statically analyze the behavior of a program, such as its resource consumption and communication protocols.

### Internship goal

To enhance the security of this critical component, we envisage encoding the type holding sensitive data using linear types. Linear types guarantee that their values are used only once; thus, they can be used to statically analyze the behavior of programs, such as resource usage and communication protocol.

In particular, the internship involves studying a recent paper “Lightweight linearly-typed programming with lenses and monads”¹ to catch at eventual secret leaks at compile time, encoding a lock-and-wipe system to make sure secrets are never written to disk, and to integrate this library into the current Tezos client implementation.

Possible challenges: - Learning about the encoding of linear types in OCaml using lenses and monads. - Learning about possible secret leaks scenarios. - Learning and modifying the code base of Tezos. - Creating and designing a formal specification of the encoding of secrets using linear types.

### Requirements

The successful applicant should have knowledge of the OCaml programming language and have attended an introductory course in type theory.

The student will work with the Nomadic Labs core development team.

### Internship Context

The intern will work at the Nomadic Labs’ offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).

Bring Michelson Coq smart contract model to the web

*Tutors: Raphaël Cauderlier, Julien Tesson*

Blockchains are decentralized ledgers, managed using a distributed peer-to-peer network. Tezos is a blockchain and a smart contract platform, developed with a focus on governance and security.

Michelson is the smart contract language used by Tezos. It is a low-level stack-based language with high-level primitives. It was built with the goal of allowing smart contracts to be formally proven with the aid of semi-automated theorem provers, such as Coq.

The Mi-Cho-Coq¹ project, developed at Nomadic Labs, provides formal semantics for Michelson programs together with weakest precondition calculus implemented in Coq.

**Internship goals**

This project focuses on bringing the Mi-Cho-Coq project to the web, by using Js-Coq², and ultimately providing a ready-to-use framework to design and present specifications of smart contracts with their proofs.

If time permits, this work can be linked to the try-michelson project³, to provide a full solution to writing, simulating, proving Michelson contracts on an easily accessible online service.

**Challenges**

Apart from the technical challenges related to the deployment of an online service, the possible challenges of this project are:

- to learn to use and install JsCoq.
- to integrate Mi-Cho-Coq in JsCoq, to provide it as a predefined theory.
- to add helpers and pre-defined structures to ease the proof of Michelson smart contracts.
- to work on an easy-to-explore library of existing smart contract and their Coq proofs, which can be used as a show case for Mi-Cho-Coq.
- to link the Mi-Cho-JSCoq service to try-michelson.

**Requirements**

The successful applicant should already be familiar with OCaml, and have a taste for web-design. Previous practice of proof-assistants would be a plus.

The student will work closely with the Mi-Cho-Coq and Tezos developers at Nomadic Labs.

**Internship Context**

The intern will work at the Nomadic Labs' offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue, gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).

---

¹https://gitlab.com/nomadic-labs/mi-cho-coq/
²https://x80.org/rhino-coq/
³https://try-michelson.tzalphp.net
Michelson by Example
Interactive, web-based, learning resources for smart contract programming

Tutor: Pietro Abate, Alexandre Doussot

Nomadic Labs is the principal developer of the Tezos blockchain. Some of the main advantages of Tezos are a strong focus on formal verification and the support of smart contracts: small programs deployed on the blockchain that implement financial software.

Smart contracts for Tezos are written in Michelson\(^1\), a stack-based language inspired by Forth, Scheme, ML, and Cat. However, trying Michelson programming requires installing OCaml and Tezos. Furthermore, there are currently no beginner-friendly tutorials for learning Michelson available online.

**Goal**

This internship is the continuation of an earlier development of a web-based interpreter for Michelson, which considerably eases the entry to Michelson.

The goal of this continuation is twofold. First, to make the web-based Michelson interpreter embeddable into other web pages. This would allow authors to demonstrate, in the browser, how Michelson contracts execute on their pages.

Second, to develop an online, example-based, learning resource for Michelson programming, inspired by the “Rust by Example”\(^2\) web page. This tutorial would leverage the embeddable interpreter for executing examples. Additionally, the tutorial can provide exercises that can be corrected automatically in the browser.

If time permits, the tutorial could also introduce formal specification and verification of smart contracts in the same vein as the “ACSL by Example”\(^3\) tutorial for specifying and proving C programs. The intern would then connect to a parallel internship at Nomadic Labs that aims to develop a web-based deductive verification tool for Michelson, based on Coq.

**Challenges**

Apart from the technical challenges related to the deployment of an online service, the possible challenges of this project are:

- Learning how to write Michelson smart contracts, and the pitfalls thereof.
- Developing tutorial material for Michelson with a suitable learning curve.
- Linking the “Michelson by Example” service to try-michelson and, potentially, JSCoq for deductive verifications.
- Learn and teaching how to formally specify and prove Michelson programs.

**Requirements**

The successful applicant should already be familiar with OCaml and have a taste for pedagogy. Knowledge of ReasonML would be a plus, but not essential (try-michelson is written in ReasonML).

**Internship Context**

The intern will work at the Nomadic Labs' offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).

\(^1\)http://tezos.gitlab.io/whitedoc/michelson.html
\(^2\)https://doc.rust-lang.org/rust-by-example/
\(^3\)https://github.com/fraunhoferfokus/acsl-by-example
Create OpenAPI based specification for Tezos

tutors: Pietro Abate, Romain Bardou

OpenAPI is a standard format to describe REST APIs. It is widely used by many projects, and many tools exist that use this specification either to create documentation, or to automatically create bindings in many different programming languages.

We have developed a Proof of Concept library to generate the OpenAPI specification of all Tezos services.

**Internship goal**

The goals of this internship are:

- to complete, test and integrate this library into the Tezos code base.
- to use the generated specification to complete the documentation of the RPC interface of a Tezos node.
- to use the generated specification to automatically create bindings for different programming languages such as Python, Rust, Kotlin, and Swift.
- to contribute to the binding generators (currently based on OpenAPI 2.0), so that they can work on version 3.0.

**Challenges**

This internship presents many technical challenges. First the students need to learn the RPC interface of Tezos and be able to extend it to automatically generate OpenAPI endpoints. This will require knowledge of the OCaml programming language and a willingness to learn the Tezos build system.

Second, the student will learn how to use automatic documentation generation frameworks and, if necessary, fix potential problems and bugs. The generated documentation should also contain examples, some of which can be generated automatically; others will require a human designer.

Finally, in order to generate bindings for different programming languages, the students must be able to quickly familiarize themselves with several different programming paradigms and learn how to best design library interfaces for these languages.

**Requirements**

The successful applicant should have a basic knowledge of the OCaml programming language. Knowledge of Python, Rust, Kotlin/Android SDK, and/or Swift/OSX is a plus, but not essential.

The student will work with the core development team and the mobile team.

**Internship Context**

The intern will work at the Nomadic Labs’ offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Protocol testing environment

Tutors: Mathias Bourgoin, Julien Tesson

Blockchains are decentralized ledgers managed using a distributed peer-to-peer network.

Different entities can interact with/within this network: nodes that replicate the state of the ledger, validators that handle the validity of operations and aggregate them into blocks, etc. When nodes diverge on the chain (producing forks) because of network latency or other technical difficulties, the consensus protocol of the blockchain makes sure that they will reach a consensus on which fork is to be the canonical chain after a small number of blocks have been aggregated. The protocol is thus responsible for the validation of blocks, but also of every transaction sent to chain.

Tezos is a self-amending ledger: it can update its consensus protocol seamlessly through an on-chain voting process. This makes it a blockchain that can upgrade this key component quickly and benefit from all the advances in the field as soon as possible. However, to test their novel ideas, protocol developers need tools; in particular they need to be able to easily deploy a test chain with their new protocol and evaluate its behavior.

Internship goals

The goal of this internship is to develop a turnkey tool to design and deploy a protocol development environment for Tezos. First, it should allow the easy definition of a genesis block (which initializes the initial accounts on the blockchain and their rights) and the properties of the chosen consensus algorithm. It should allow the deployment of different nodes and validators, compatible with the new protocol, on a heterogeneous network. Finally, it should be usable for evaluating the behavior of the resulting chain.

Requirements

The intern should have a working knowledge of OCaml programming.

Internship Context

The intern will work at the Nomadic Labs’ offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Zero Knowledge Proof Scheme Implementation

*Tutors: Marco Stronati, Marc Beunardeau*

Blockchains are decentralized ledgers managed using a distributed peer-to-peer network. Tezos is a blockchain and a smart contract platform, which development focus on governance and security.

**Internship goals**

This internship aims to implement a zero-knowledge prover in Ocaml and a verifier in Michelson, the smart contract language of Tezos.

We have integrated a zero-knowledge prover and verifier for a specific program into Tezos, which allows us to make anonymous transfers. The schema behind the prover-verifier pair gives us efficiency but comes at the cost of a trusted setup. We would like to have the option of adding a few provable properties to our anonymous transactions (e.g. whether the money comes from a whitelist). For this, we would need another program, meaning that we would need a trusted setup for each specific application. We can get around this by using trust-less setup zero-knowledge schemes, which will be implemented during the internship.

**Outline**

The internship will be divided into two main parts. First, the intern will select a zero-knowledge scheme that best fits our purpose. This first part will consist mainly of becoming familiar with the state-of-the-art zero-knowledge proofs and their different trade-offs, as well as Tezos’ specific needs. The second part will consist of implementing the chosen scheme. The prover and setup will be done in Ocaml and integrated into Tezos’ code base.

The verifier will then be integrated in Michelson, which will first require the development of an elliptic curve library for Michelson.

**Profile**

The intern should have a good background in Ocaml, and a basic background in algebra and cryptography. The intern should be able to work independently, understand academic papers and the purpose of their work will be to propose solutions to the different problems they will encounter independently. They will be guided through the Tezos code-base, Michelson language, blockchain-specific problems and zero-knowledge proofs in general.

**Internship Context**

The intern will work at the Nomadic Labs’ offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).
Zero Knowledge Proof for Off-Chain Computation

Tutors: Marco Stronati, Marc Beunardeau

Blockchains are decentralized ledgers managed using a distributed peer-to-peer network. Tezos is a blockchain and a smart contract platform, developed focusing on governance and security. Smart contracts are re-executed by each node in the network to verify the integrity of the computation. This imposes a strict limit on the resources each contract can use in terms of storage and computation (gas). In principle, only a proof of the correctness of the execution needs to be checked and, for complex programs, this verification could be cheaper than re-execution. Several zero-knowledge proof schemes offer “succinct” proofs that are small in size with respect to the program and have fast verification times. Being zero-knowledge, the same proofs can be used to protect the confidentiality of the computation or of its data.

Internship goals

The purpose of this internship is to use ZK-proofs to prove on-chain the integrity of off-chain computations, the computations being arbitrarily defined by the user or chosen from a set of templates.

Outline

The first part of the internship will be devoted to familiarization with the Tezos blockchain and the state-of-the-art in zero-knowledge proof schemes for off-chain computations. Promising works are Zexe and ZoKrates. Additionally, a few reference applications will be designed.

In the second part, the student will implement the chosen scheme as an OCaml library, to be used by one of the high-level languages for smart contracts for Tezos (LIGO, SmartPy). One or more of the reference applications will be implemented on top of the library.

Profile

The intern should have a working knowledge of OCaml. Familiarity with Rust would be a plus. Basic understanding of elliptic curve cryptography and zero-knowledge proofs are good additions. The intern should be able to work independently, understand academic papers, and propose solutions to the different problems encountered.

Internship Context

The intern will work at the Nomadic Labs’ offices in Paris or Grenoble.

Participating in a large scale open-source project they will have to rapidly learn to use collaborative tools (git, merge request, issue gitlab, continuous integration, documentation) and to communicate about their work. The final work might be presented at a conference or a workshop with an international audience.

The intern, who will have a designated advisor at Nomadic Labs, will have to work independently and to propose thoroughly considered solutions to the different problems they will have to solve. However, they 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).