# An Introduction to Zero Knowledge Proofs

## Description

Zero-knowledge proofs (ZKPs) offer a unique combination of privacy and verifiability in digital transactions. During this beginner-friendly workshop, we will learn what a ZKP is and how to integrate it into common web applications. In the end, you will have all the complete tools to masterfully use ZKPs in your own projects!

## Learning Outcomes

After this workshop, you will be able to:

- Conceptually understand ZK proofs
- Understand the use of ZK in privacy-enhancing technology
- Build simple applications that utilize zero knowledge proofs

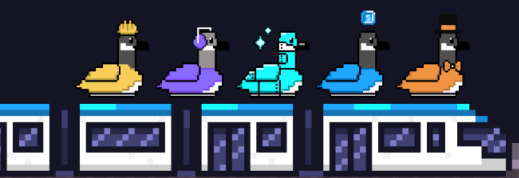
## Prerequisite Knowledge

- Familiarity with a general programming language (c/c++, JS, python, etc)
- Familiarity with navigating a unix-based operating system

## Pre-Workshop Checklist

Before the workshop, please make sure you complete the following items:

- Check out the github repository that we will use for the tutorial
- Prepare a local clone of the exercise branch in a unix environment
- Optional: under the read.me, install any missing dependencies ahead of the workshop



## Technical Jargon and Definitions

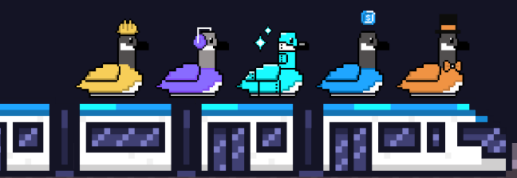
- **Zero Knowledge Proofs:** Cryptographic techniques that allow one party to prove to another they know specific information without revealing the actual information.
- **ZK-SNARK**: A form of zero-knowledge proof that is both succinct (short and quick to verify) and non-interactive (requiring no back-and-forth communication between the prover and verifier).
- **Circom:** A domain-specific language and toolkit for creating efficient zero-knowledge proof circuits, especially used in zk-SNARK implementations.

## Timeline (1 hour)

| Time | Module | Description |
|---|---|---|
| 10 min | ZK intuition | What even is a ZK proof? |
| 5 min | Note on privacy | How does ZK apply to privacy? |
| 5 min | Building on zk | What does the tech stack look like? |
| 40 min | ZK app tutorial | A complete end-to-end web app using ZK |

## Workshop Lead Contact


| Markos Georghiades |
|---|
| markos@quantstamp.com |

## Additional Resources

### Hack the North Resources

Hack the North 2023 Event Schedule

Check this out to stay up-to-date on activities, workshops, and other key happenings this weekend.

### Workshop-Specific Resources

0xparc ZK learning resources

One of the best resource hubs for ZK learning content and lectures.

Github Repository

Full repository for this workshop. Contains the exercise boiler and solution.