

REPORT DRAFT FOR MASTER'S THESIS

Implementation and Evaluation of Programmable Money
Using Verifiable Credentials and Zero-Knowledge Proofs

Yat Wai Wong

Supervisor:

Prof. Wolfgang Prinz, PhD

Prof. Stefan Decker, PhD

Date

RWTH Aachen University

Contents

1	Things to be included in the report	2
---	-------------------------------------	---

1 Things to be included in the report

- Third party library cannot be controlled, e.g.,
sometimes metamask not working
sometimes privado not working
- Using Privado's web wallet to generate proof: no way to log proof generation time,
e.g. no api for that, cannot change their code.
possible solution to track proof generation time is to use selenium
- using metamask vs transaction done on backend: users trust metamask vs trust
our backend