

Building a Blockchain Library for OCaml

Charlie Crisp, Pembroke College

October 12, 2017

Project Supervisor: KC Sivaramakrishnan

Director of Studies: Anil Madhavapeddy

Project Overseers: Timothy Jones & Marcelo Fiore

1 Introduction

Blockchain technology has generated a lot of interest in recent times, but mostly in the field of cryptocurrencies. With a simple Proof of Work consensus algorithm, the blockchain can be used to build a distributed ledger of transactions which is only vulnerable to attack, when more than half of the workforce is fraudulent.

I will build a pure OCaml, reusable blockchain library to allow the creation of distributed, secure ledgers, which are agreed upon by consensus. The library will allow for the creation of blockchain applications outside the scope of cryptocurrencies.

It will be built on top of Irmin [1] - a distributed database with git-like

version control features. Being pure OCaml, the blockchain nodes can be compiled to unikernels or JavaScript to run in the browser. I will evaluate the blockchain by prototyping a decentralised lending library and evaluating the platform's speed and resilience.

2 Starting point

The project will build upon functionality provided by Irmin [1] which is a distributed database system.

THIS IS COPIED FROM <https://mirage.io/blog/introducing-irmin>

Irmin is a library to persist and synchronize distributed data structures both on-disk and in-memory. It enables a style of programming very similar to the Git workflow, where distributed nodes fork, fetch, merge and push data between each other. The general idea is that you want every active node to get a local (partial) copy of a global database and always be very explicit about how and when data is shared and migrated..

3 Resources required

4 Work to be completed

5 Evaluation criteria

6 Timetable

7 References

References

- [1] Irmin - A pure OCaml, distributed database that follows the same design principles as Git.
<https://github.com/mirage/irmin>