Bern University
of Applied Sciences

Project 2

Bitmessage – Communication Without Metadata

Author Christian Basler
Tutor Kai Brünnler
Date April 30, 2015

Contents

1. Synopsis

TODO

2. Basics

While encryption technology like PGP or S/MIME provides a secure way to protect content from prying eyes, ever since Edward Snowdens whistleblowing we learned that metadata — most notably information about who communicates with whom — is equally interesting and much easier to analyze.

With e-mail, we can only prevent this by encrypting the connection to the server as well as between servers. Therefore we can only hope that both our and the recipient's e-mail provider are both trustworthy as well as competent.

With Bitmessage we send a message to a sufficiently large number of participants, with the intended recipient among them. Content is encrypted such as only the person in possesion of the private key can decrypt it. All participants try to do this in order to find their messages.

The protocol is described in detail in my Seminar paper.

3. Goal

At the moment, there aren't many implementations apart from the official clients. Especially two things are missing: a multi purpose Java library and a usable mobile client. My goal for my *Project 2* is to create the library, to be used next semester as a starting point for an Android™ client in my Bachelor Thesis.

4. Issues

TODO

4.1. Unsigned Numbers

Java doesn't support unsigned number types. While Java 8 has some helper classes to address this issue, my goal is to support Java 7, which is needed for Android development, so I wasn't able to leverage them.

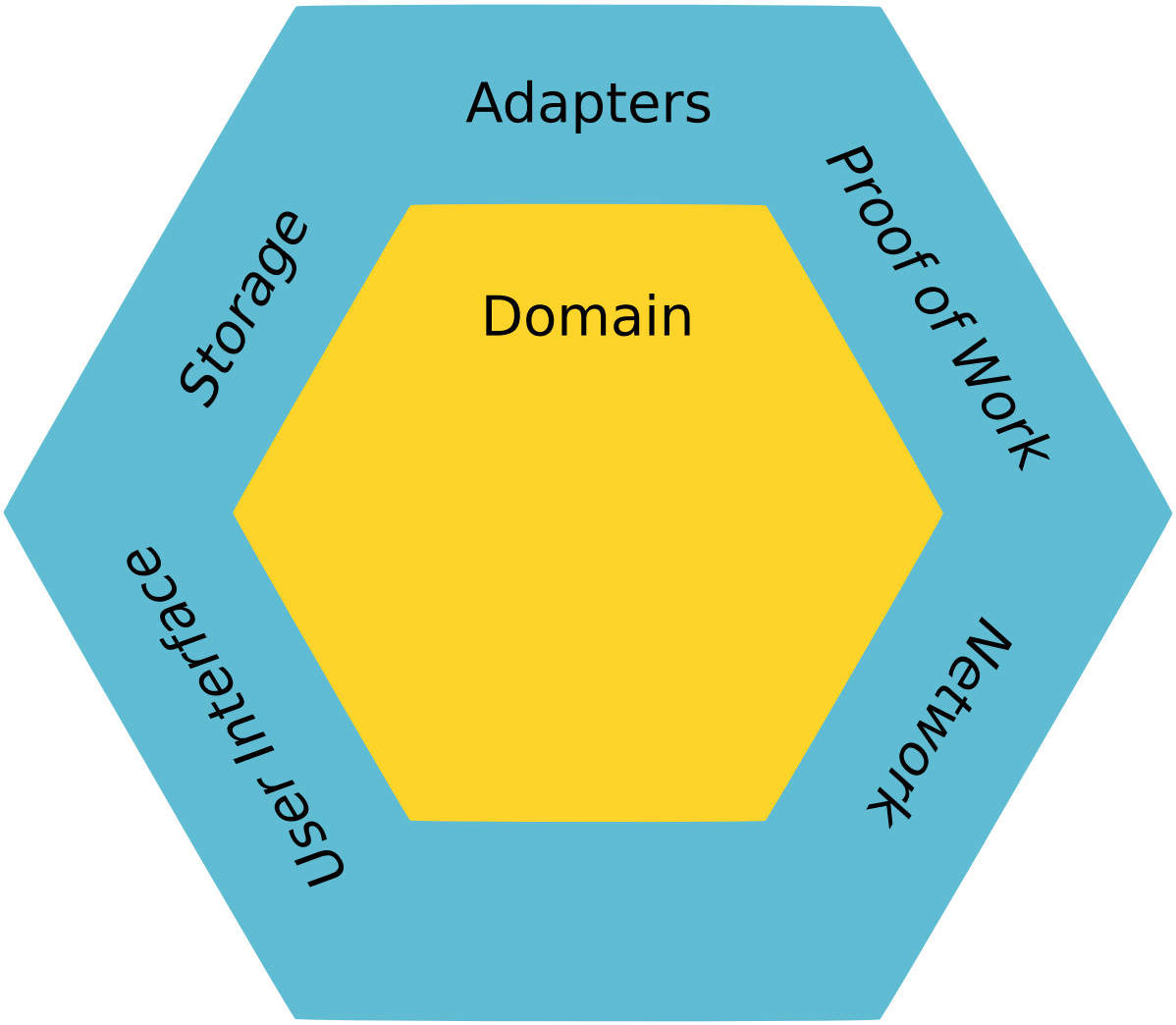
4.2. Proof of Work

Proof of work is needed for a message to be distributed within the Bitmessage network. This is to protect both the network itself from denial of service attacks and the users from spam.

5. Architecture

5.1. Ports and Adapters

The library uses a ports and adapters architecture, which allows us to easily replace some implementations that might be platform dependent, such as storage or proof of work calculation.



The big advantage of this approach is that it's easy to test the core as well as each adapter by itself.

5.2. Network Management

6. Usage

TODO

7. Discussion

Appendix

A. JavaDoc Documentation

B. Literature