Bern University
of Applied Sciences

Bachelor Thesis

Android Client for Bitmessage

Author	Christian Basler
Tutor	Kai Brünnler
Date	June 18, 2015

Contents

1 Project Setup

1.1 Current state – why is it bad?

Until recently there was not mobile client for the Bitmessage protocol, and the client that turned up since is very wasteful to the devices resources, draining the battery in no time.

1.2 How should it be?

We need mobile Bitmessage clients that allows the user to choose the levels of convenience, privacy and resource hunger.

1.3 Why is it hard to do?

Bitmessage is very wasteful with resources by design. All messages are being sent to and stored on all nodes, and to protect the network a proof of work (POW) is required for all objects that are distributed.

1.4 How do I intend to do it?

As I developed Jabit, a Java implementation of the Bitmessage client, as my last project, I have great knowledge about the Bitmessage protocol. There are a few optimisations that I intend to do;

- Connect to only one reliable node instead of eight random nodes
- Don't save objects we can't decrypt
- Only connect to the network if we're on Wi-Fi and charging

Of course every option has its own drawbacks, so they will be configurable. As for the POW: Jabit highly optimises its calculation, which might be enough for modern smartphones.

Further optimisations might introduce a server component that might do

- POW
- Request public keys, requiring us to give up some anonymity towards the server.
- Inform the client about new messages sent to its addresses. This would mean to give up our anonymity towards the server in the best case (which isn't supported by the protocol yet), towards the whole network (which is somewhat supported), or give up the private key to the server (which is just a big NOPE).