What is it about?

If you don't want anyone snooping around your e-mails you might already encrypt your correspondence. But you still can't hide who you're writing to. Your e-mail client might even reveal much more about you, your computer, and the software you use.

Bitmessage attempts to solve all this, but up until now there was no practical way to use it on mobile phones.

A big advantage of Bitmessage is its inherent key management. The address contains a hash of the public key, and retrieving said key is an integral part of the protocol. The way addresses look ensues:

`BM-2cWs84ik1Fj7jdJKrn3vDecxQbH9R4VS9r`

*Visit **dissem.ch/abit** for more information about the app*

Bitmessage

Bitmessage is a peer to peer messaging protocol that builds a mesh network among the participating clients. Each client tries to maintain multiple connections to other network nodes and has an encrypted copy of every current message.

There are some unique challenges for mobile clients:

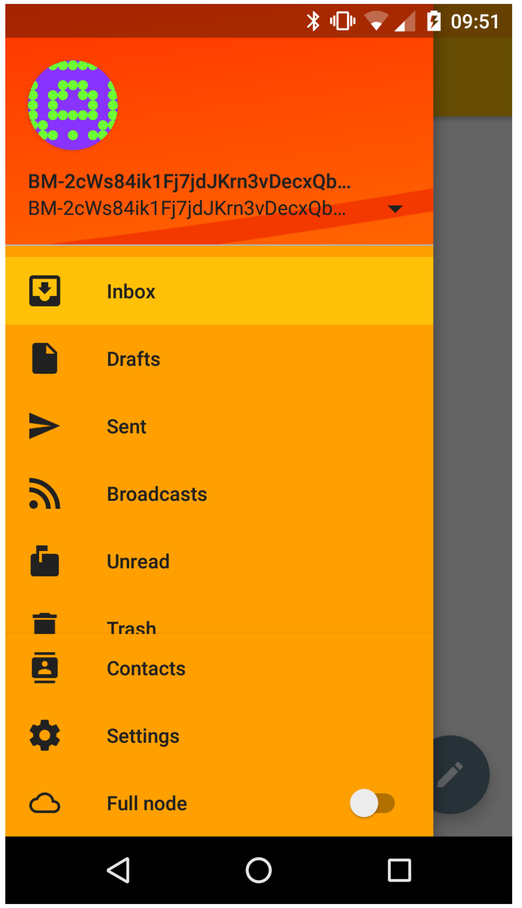
- its users are very privacy conscious
- the protocol needs huge amounts of traffic
- and a lot of CPU time

It works by distributing every message to every client, so they can pick up the ones they can decrypt with the available private keys.

To protect the network from malicious flooding, a proof of work is required, which is done by calculating a partial hash collision. This is designed to be relatively slow even on desktop computers.

To do all this you probably want as many CPU cores as possible, no shortage of electricity and a flat rate on internet access – not quite the perfect basis for a mobile app.

The Result



Abit looks just like any e-mail app, apart from the look of Bitmessage addresses and the switch called ‘full node’ at the bottom, which starts the connection to the network.

If a so called ‘trusted node’ is defined in the settings, it will periodically check for new messages even without the full node running.

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

An Android Client for Bitmessage

▶Bachelor Thesis 2015/16 Division of Computer Science

Graduate: Christian Basler
Professor: Dr. Kai Brünnler
Expert: Daniel Voisard