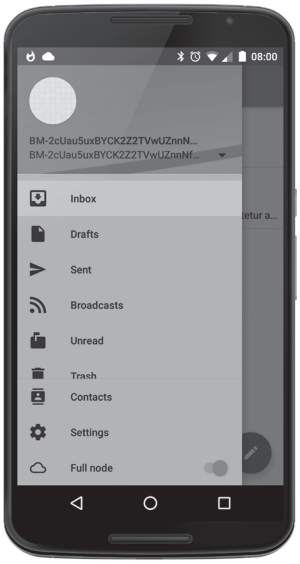
Bitmessage for Android

Degree programme: BSc in Computer Science | Specialisation: Mobile Computing
Thesis advisor: Dr. Kai Brünnler
Expert: Daniel Voisard (BAKOM)

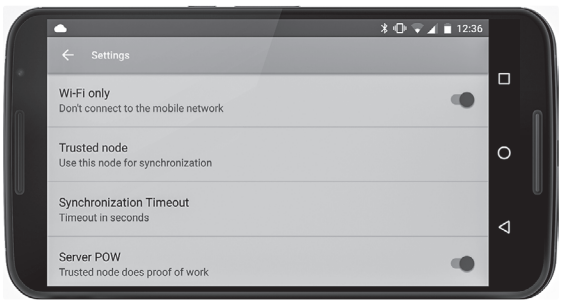
Even if you are encrypting your e-mails, you still can't hide who you're writing to. Your e-mail client might even reveal much more about you, your computer, and the software you use.
Bitmessage solves all this, but up until now there was no practical way to use it on mobile phones. That's where this thesis comes in.

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. For one, its users are very privacy conscious. Also, the protocol needs both 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, clients must find a partial hash collision as proof of work in order to send a message. This is designed to be relatively slow even on desktop computers.



So typically you'd want as many CPU cores as possible, no shortage of power and a flat rate on internet access – a challenge for a mobile app.
Android has some challenges, too. To preserve resources, the operating system might kill any process at any time, especially those in the background that process incoming network objects. Then there are some major Java dependencies missing in the Android VM, most notably JDBC, used to access databases. And finally, the devices differ vastly in processing power. The implementation we propose solves these problems.
In addition there were two optional optimisations that require a server. First, Android provides a highly optimized method to synchronize data with a server, which we leveraged while still using the official Bitmessage protocol. Secondly, an option to let a server do the proof of work was added for weaker phones. For both options the user must give up some of his anonymity towards the server – the choice is theirs.

You can get more information about the app at
dissem.ch/abit



Christian Basler