Waku - P2P Messaging for resource restricted devices

oskarth

February 3, 2020

Abstract

such abstract, much abstraction

1 Introduction

Whisper is a peer-to-peer messaging protocol that was created as part of the Ethereum project. It was meant as one of the three legs of the world computer, the other two being compute/consensus (Ethereum itself) and storage (Swarm). [ref]

However, it hasn't seen a lot of uptake. One project that used this is the Status mobile app [ref]. There are many fundamental issues with Whisper, especially when it comes to running on resource restricted devices.

Our contribution is the Waku protocol, which is a fork of Whisper that solves some of the key problems seen with the Whisper protocol when running on resource restricted devices such as mobile phones with limited data plan. These specific problem areas and contributions can be summarized as follows.

A resource restricted device is restricted in several ways. Here we list the most relevant for mobile phones, with a brief summary of how we address them:

1. Mostly-offline: Users on mobile phones are usually mostly-offline, and have limited connection windows. This is addressed be the use of an *offline inbox* protocol.

2. Limited bandwidth: Users on mobile phones usually have a limited data plan, and Whisper scales extremely poorly by default. We address this in various ways.

3. Limited battery: Whisper uses *proof of work* as a spam mechanism, which works poorly on mobile phones. We address anti-spam in other ways. Additionally, we limit connectivity in a light node fashion.

The main ”ping” or idea is making Whisper run on resource restricted device. That's the game.

TODO: Right now this doesn't clarify why we want something like Whisper in the first place

2 Problem

Offline, BW, Spam.

3 Idea

4 Details

Scalability model, simulation.

Status app as a case study?

5 Related work

Whisper, PSS, Bitmessage, similar P2P routing.

6 Conclusion and future work

TODO: This should highlights of things to come for next version

- more efficient routing (but also sup logical centralization - stronger privacy guarantees, better trilemma position (mixnet) - run on libp2p more devices etc - spam resistance better

7 References

8 Notes

- But why should anyone care about Whisper? What happens if we imagine Whisper didn't exist?

  - Why p2p in the first place?