A TrustChain Approach for Smartphones

Measuring reconnection latency when the network is interrupted

Author: Alexandra Nicola
Supervisors: Johan Pouwelse, Bulat Nasrulin

TU Delft

1. Introduction

- **Why blockchain?** Traditional blockchains are often heavy, energy-intensive, and poorly suited for mobile devices
- **Our focus:** Explore TrustChain[1] a lightweight, P2P blockchain architecture optimized for smartphones.
- Implement and evaluate TrustChain's potential on mobile phones, using different network protocols.

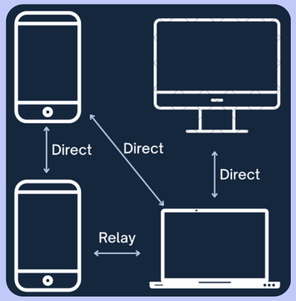
2. Research question

How can a smartphone-optimized implementation of Trustchain be built from scratch to support real-time P2P communication?

Optimization focus: How **robust** is TrustChain, in terms of reconnection latency, when running over different network protocols?

3. Methodology

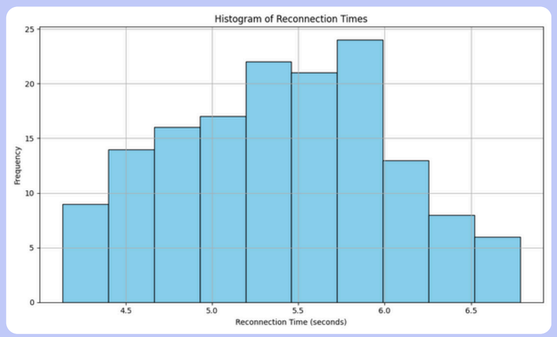
- Analyze network protocols: UDP, Iroh over QUIC[2], Kotlin IPv8, TFTP[3]
- Exchange UDP packets between phones
- Implement Trustchain in Rust on Android via JNI - signature verification, hashing, deduplication, timeout handling
- **Networking** layers implemented:
  - Raw UDP mode → simple, stateless, sequence numbers, timeouts, deduplication
  - Iroh[2] over QUIC (via Quinn library) → secure, public key-based peer discovery, direct or relay-based connections
- **Experiment**: simulate Wi-Fi interruption and measure reconnection latency
  - Wi-Fi enable/disable via ADB shell commands
  - 150 automated test runs per protocol
  - **Reconnection latency** = time between network restoration and receipt of the first valid TrustChain message
  - Compare reconnection time for UDP and Iroh over QUIC



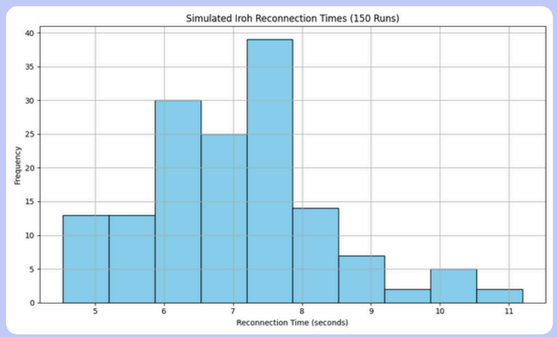
IROH

4. Results

- UDP - consistent reconnection, 4-6 seconds, ~5s average
  - Underlying OS-level latency: Wi-Fi initialization, IP address assignment
- Iroh over QUIC - variable reconnection, 4.5 - 11.5s, peak 6 - 8s
  - Slower due to QUIC timeout detection, DNS discovery, relay handshake



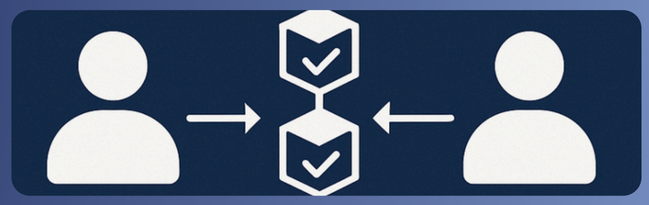
UDP, 4-6s



IROH, 4.5-11.5s

5. Analysis

- Simpler ≠ worse: UDP's lack of recovery logic achieves short drops
- Iroh over QUIC comes with performance trade-offs. Factors identified:
  - QUIC timeout: waits before giving up on the old connection, using exponential backoff (1s, 2s, 4s,..)
  - DNS discovery: has to find the peer again after coming back online, looks up peer using dynamic DNS
  - Relay reconnection: secure connection is rebuilt from scratch



6. Future work

- Change QUIC's parameters: shorten idle time-out, introduce keep-alive packets, maintain a persistent Endpoint instance, or skip the discovery step for known addresses
- Multipeer support
- Protocol switching strategies
- Different Wi-Fi congestion levels evaluation

References:
[1] Johan Pouwelse. Trustchain: A sybil-resistant scalable blockchain. 2020. InternetDraft, Internet Engineering Task Force (IETF).
[2] https://www.iroh.computer
[3] https://www.pynetlabs.com/what-is-tftp-protocol/