How it works - Briar

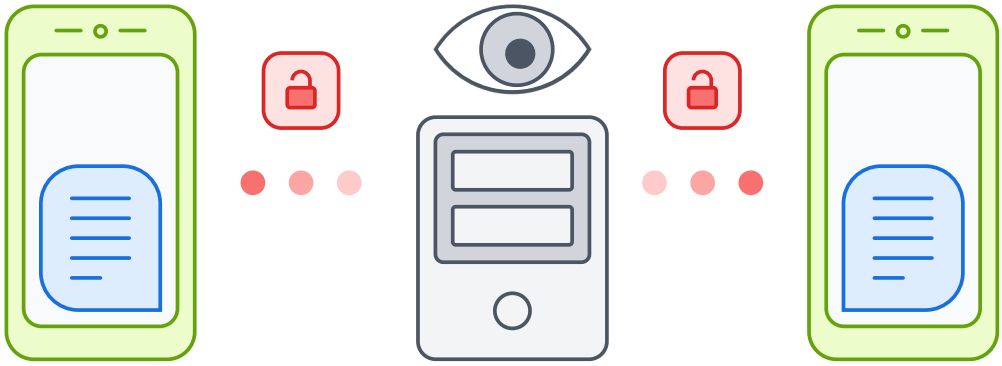
4-5 minutes

Briar is a messaging app designed for activists, journalists, and anyone else who needs a safe, easy and robust way to communicate. Unlike traditional messaging apps, Briar doesn't rely on a central server – messages are synchronized directly between the users' devices. If the Internet's down, Briar can sync via Bluetooth, Wi-Fi or memory cards, keeping the information flowing in a crisis. If the Internet's up, Briar can sync via the Tor network, protecting users and their relationships from surveillance.

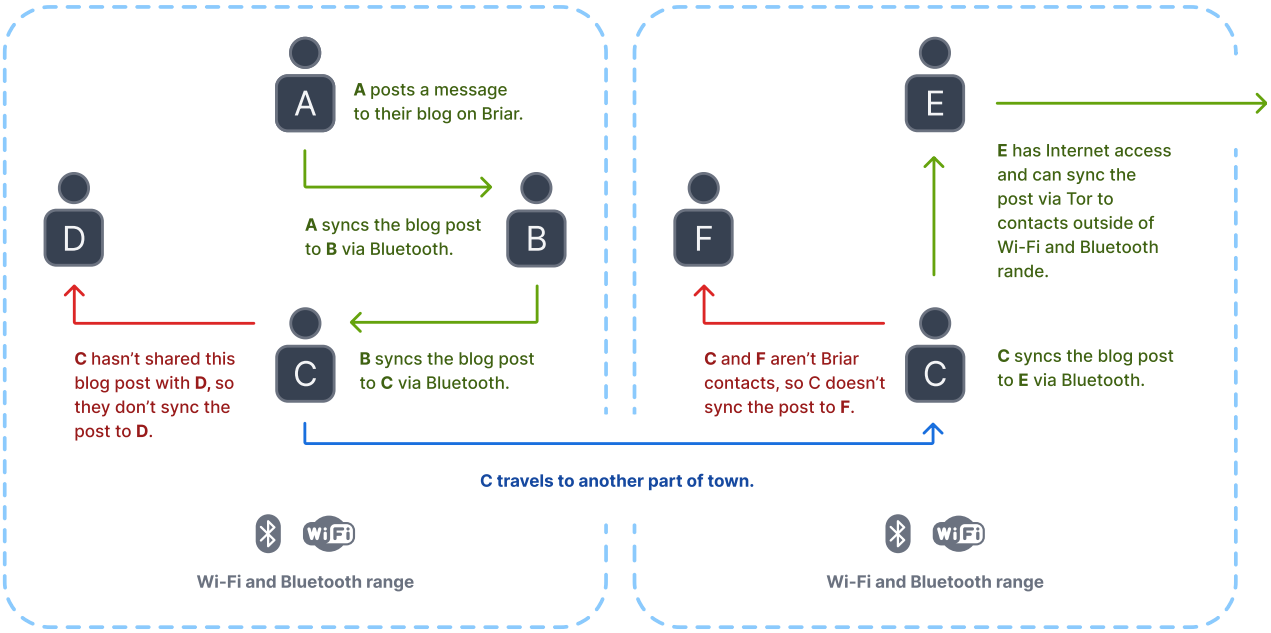
Users who are online at different times can use Briar Mailbox to deliver their messages securely.

The quick start guide and the manual describe how to use Briar and the features that are available. Technical details are available on the wiki and explained in this video.

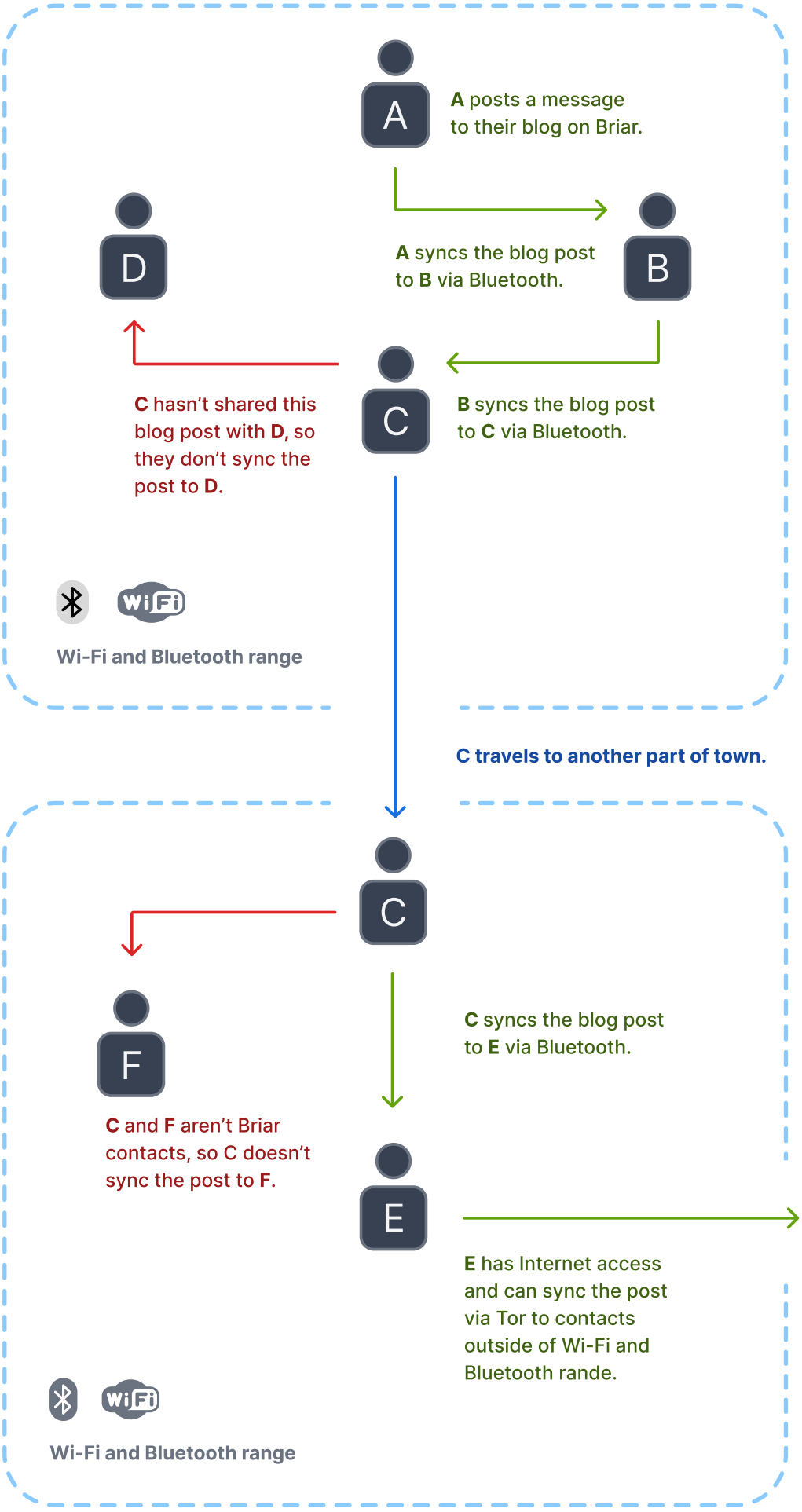
Briar uses direct, encrypted connections between users to prevent surveillance and censorship.



Typical messaging software relies on central servers and exposes messages and relationships to surveillance.



Briar can share data via Wi-Fi, Bluetooth and the Internet.


A
A posts a message to their blog on Briar.
A syncs the blog post to B via Bluetooth.
B
D
C
B syncs the blog post to C via Bluetooth.
C hasn't shared this blog post with D, so they don't sync the post to D.
Wi-Fi and Bluetooth range
C travels to another part of town.
C
C syncs the blog post to E via Bluetooth.
F
C and F aren't Briar contacts, so C doesn't sync the post to F.
E
E has Internet access and can sync the post via Tor to contacts outside of Wi-Fi and Bluetooth rande.
Wi-Fi and Bluetooth range

Briar can share data via Wi-Fi, Bluetooth and the Internet.

Briar provides private messaging, public forums and blogs that are protected against the following surveillance and censorship threats:

- **Metadata surveillance.** Briar uses the Tor network to prevent eavesdroppers from learning which users are talking to each other. Each user's contact list is encrypted and stored on her own device.
- **Content surveillance.** All communication between devices is encrypted end-to-end, protecting the content from eavesdropping or tampering.
- **Content filtering.** Briar's end-to-end encryption prevents keyword filtering, and because of its decentralized design there are no servers to block.
- **Takedown orders.** Every user who subscribes to a forum keeps a copy of its content, so there's no single point where a post can be deleted.
- **Denial of service attacks.** Briar's forums have no central server to attack, and every subscriber has access to the content even if they're offline.
- **Internet blackouts.** Briar can operate over Bluetooth and Wi-Fi to keep information flowing during blackouts.

Briar is designed to resist surveillance and censorship by an adversary with the following capabilities:

- All long-range communication channels (internet, phone network, etc) are comprehensively monitored by the adversary.
- The adversary can block, delay, replay and modify traffic on long-range communication channels.
- The adversary has a limited ability to monitor short-range communication channels (Bluetooth, WiFi, etc).
- The adversary has a limited ability to block, delay, replay and modify traffic on short-range communication channels.
- The adversary can deploy an unlimited number of devices running Briar.
- There are some users who can keep their devices secure - those who can't are considered, for the purposes of the threat model, to be controlled by the adversary.
- The adversary has a limited ability to persuade users to trust the adversary's agents - thus the number of social connections between the adversary's agents and the rest of the network is limited.
- The adversary can't break standard cryptographic primitives.

Our long-term plans go far beyond messaging: we'll use Briar's data synchronization capabilities to support secure, distributed applications including crisis mapping and collaborative document editing. Our goal is to enable people in any country to create safe spaces where they can debate any topic, plan events, and organise social movements.