

A brief introduction to Session



2020-07-16

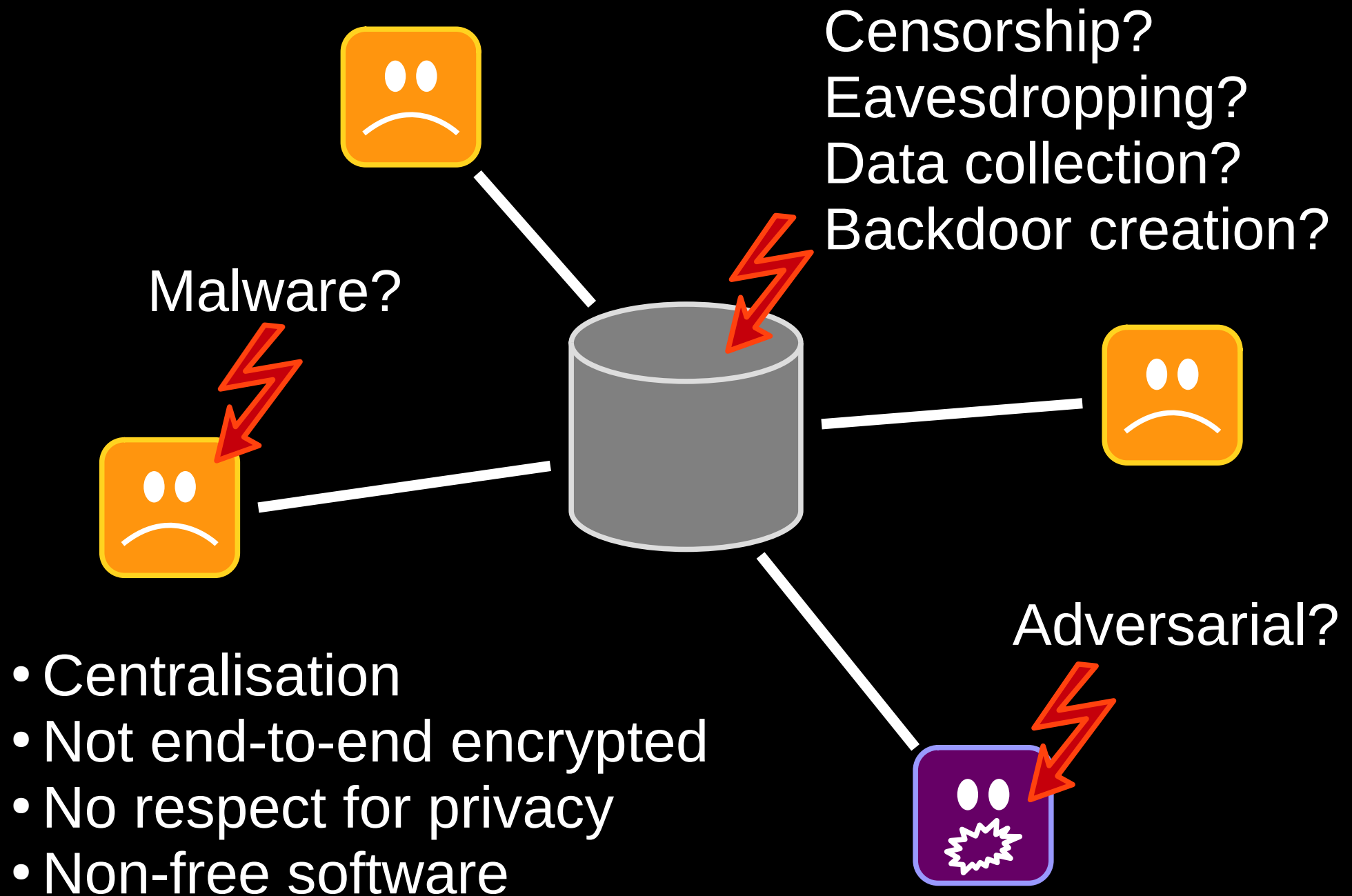
What is Session?



"Send (Encrypted) Messages Not Metadata"

- A decentralised private instant messenger
- Uses Signal protocol for encryption
- Uses onion routing for metadata resistance
- Officially launched on 2020-02-06 (version 1.0.0)
- Free software (GPL 3.0)

What's wrong with other messengers?

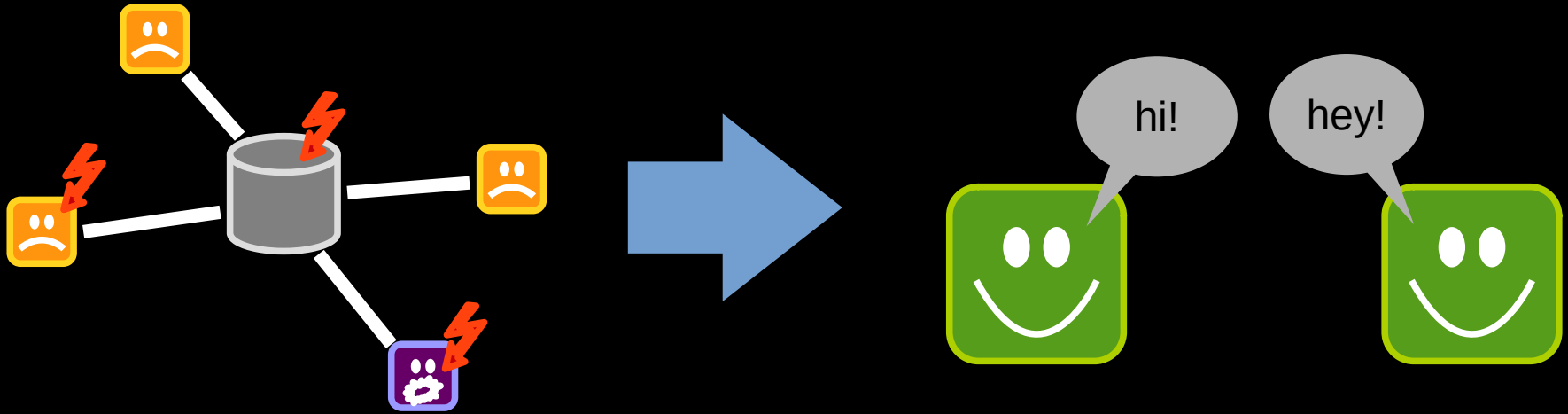


What's wrong with other messengers?



- Peer to peer
 - Anyone who chats with you gets your IP address
 - Any point along the network path knows who is chatting with who
- Centralised
 - Signal knows who is chatting with who
 - Requires a phone number
 - Requires a smartphone
 - Distributed mainly through Google/Apple

Why is Session worth attention?



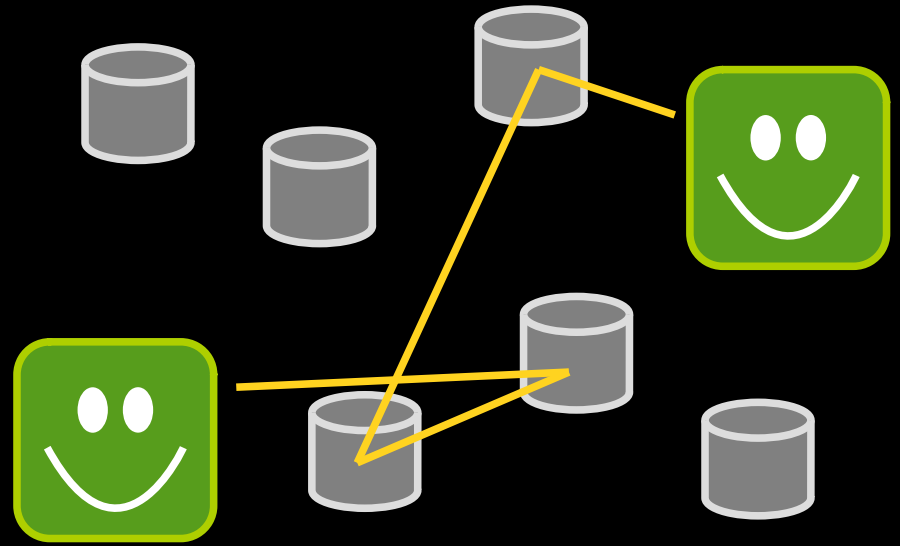
- Currently no way to chat privately on the internet
- An online analog for face-to-face chat is needed
- Session is a step forward towards private chat

What features does Session have?

~~+61 401 234 567~~



0501234567890abcdef01234
567890abcdef01234567890a
bcdef01234567890abcdef



- Public keys (66 hex string) as identifiers
- Instant messaging and file sharing
- ~~Proxy routing~~ -> onion routing -> Lokinet
- Closed groups (E2EE) of up to 10 people
- Open groups (no E2EE) hosted on servers
- Voice chat is on roadmap but requires Lokinet

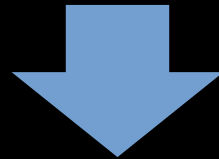
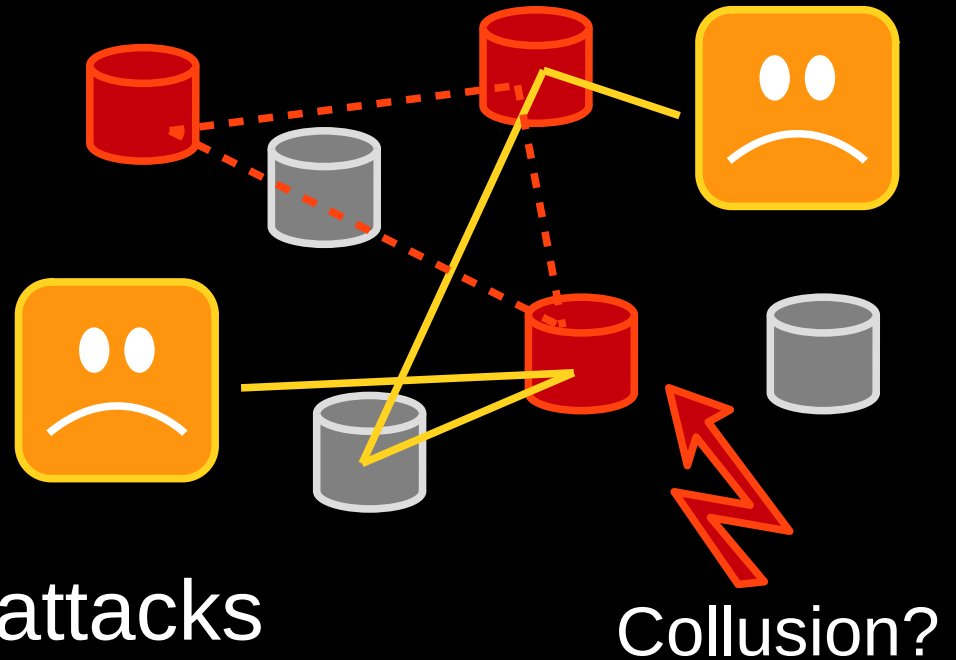
Who is developing Session?



- Loki Project, a startup in Melbourne, Australia
- The group was formed in 2018?
- Related projects:
 - Loki (cryptocurrency)
 - Lokinet (anonymity network)
- Inspiration/forks: Monero, Signal, I2P, ...

Why the Lokinet anonymity network?

- I2P's network is vulnerable to Sybil attacks
- Tor's network:
 - is vulnerable to Sybil attacks
 - cannot route UDP packets
 - is more centralised due to directory authorities



- Lokinet aims to:
 - mitigate Sybil attacks: nodes "stake" \$Loki
 - reward nodes for their service to Lokinet
 - route all IP traffic: HTTP, games, voice, ...

What are Session's limitations?

- Still under very active development, needs polishing, and may change a lot over time
- No voice/video chat yet. This requires Lokinet
- Android app not yet available on F-Droid
- Low-latency (weak) anonymity: a resourced adversary can still de-anonymise users
- Lacks translations into other human languages
- More Loki nodes and \$Loki adoption required?
- More Session users required to improve anonymity

How to get started with Session?



<https://getsession.org>

- Available as source, Deb, APK, iOS, Mac, Win
- Download binaries and PGP sigs from GitHub:
 - Desktop: <https://github.com/loki-project/session-desktop/releases>
 - Android: <https://github.com/loki-project/session-android/releases>
 - iOS: <https://github.com/loki-project/session-ios/releases>
- Verify your download, then install
- Generate your ID, securely keep your private seed
- Configure settings to your liking
- Share your ID, add your friends, start chatting
- Join some open groups (eg: chat.getsession.org)

How to contribute to Session?

- Encourage other people to use it. Share your ID
- Report issues or request features on GitHub
- Develop it and request pulls
- Run Loki nodes: <https://loki.network>
- Explore other Loki projects