Communication Applications

Being FOSS is only a first step

Welcome!

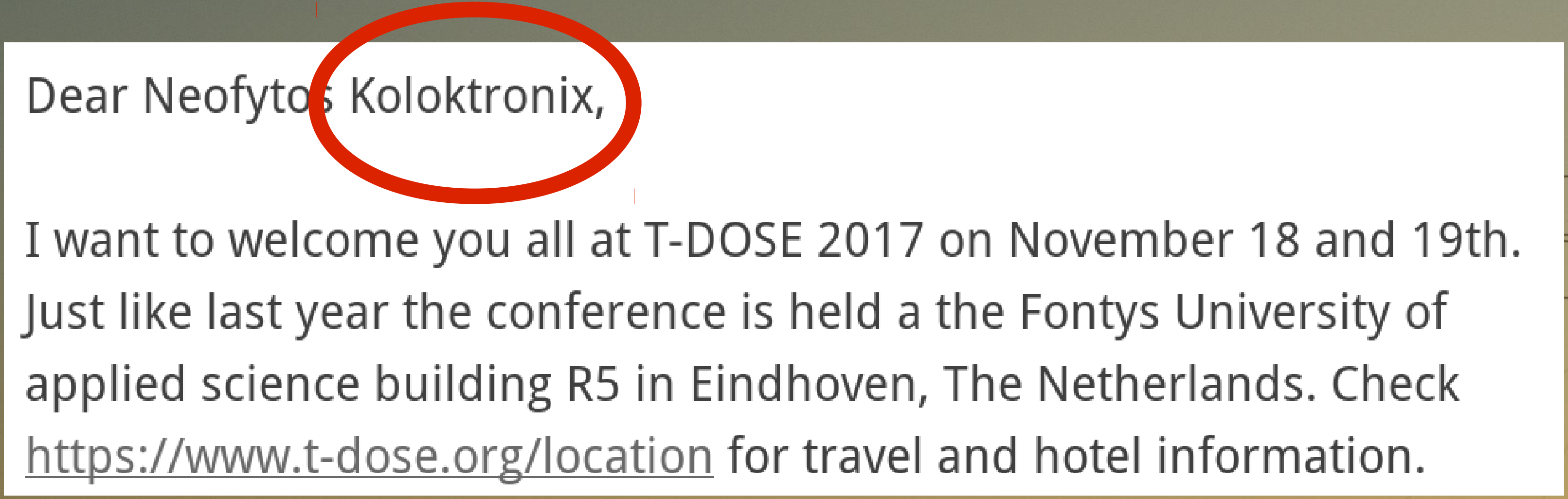
$ whoami

Neofytos Kolokotronis

Connect with me at:
https://about.me/neofytosk

$ whoami

Neofytos Kolokotronis

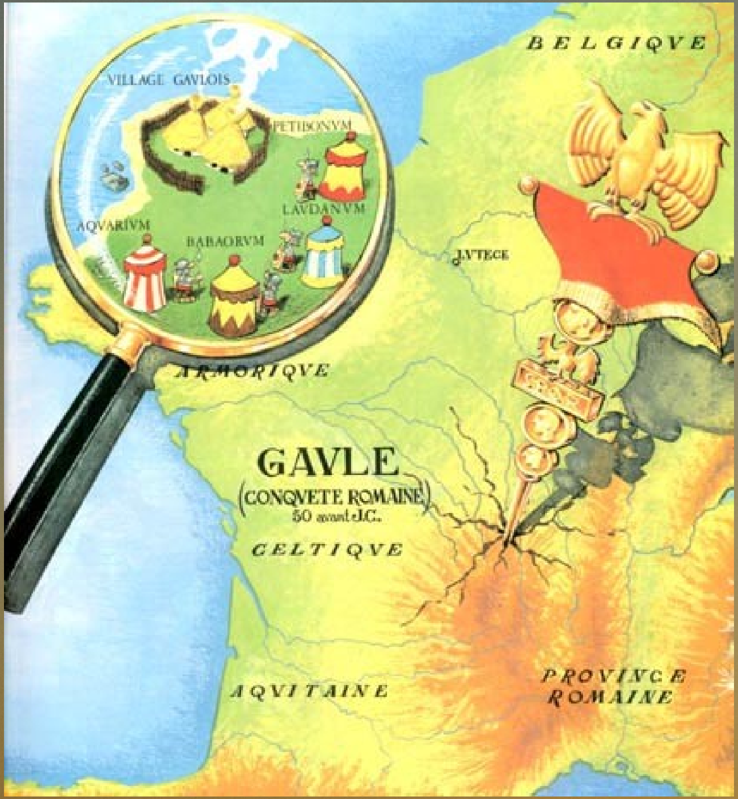


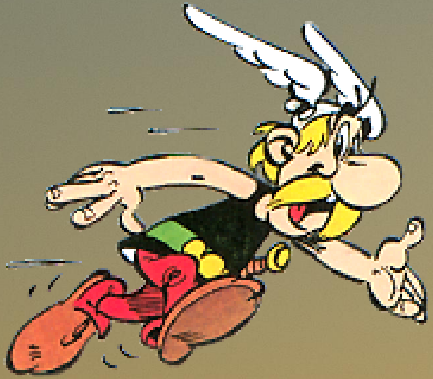
Dear Neofytos Koloktronix,

I want to welcome you all at T-DOSE 2017 on November 18 and 19th. Just like last year the conference is held a the Fontys University of applied science building R5 in Eindhoven, The Netherlands. Check https://www.t-dose.org/location for travel and hotel information.

$ whoami

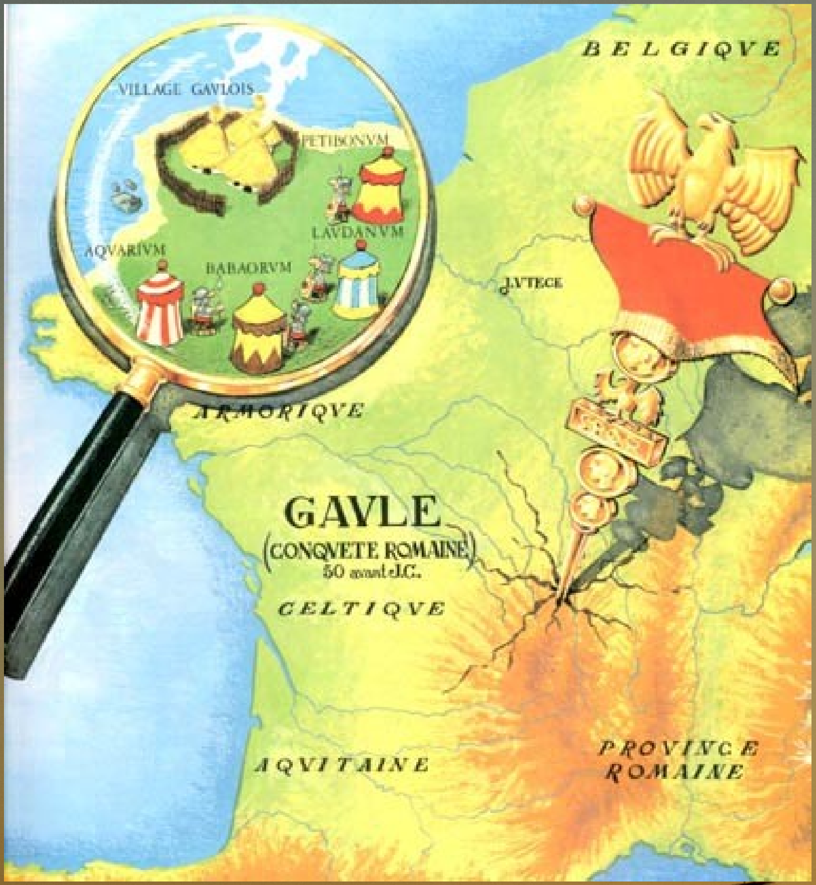
Neofytos Koloktronix?





$ whoami

Neofytos Kolokotronis



$ whoami

Just call me Neo…

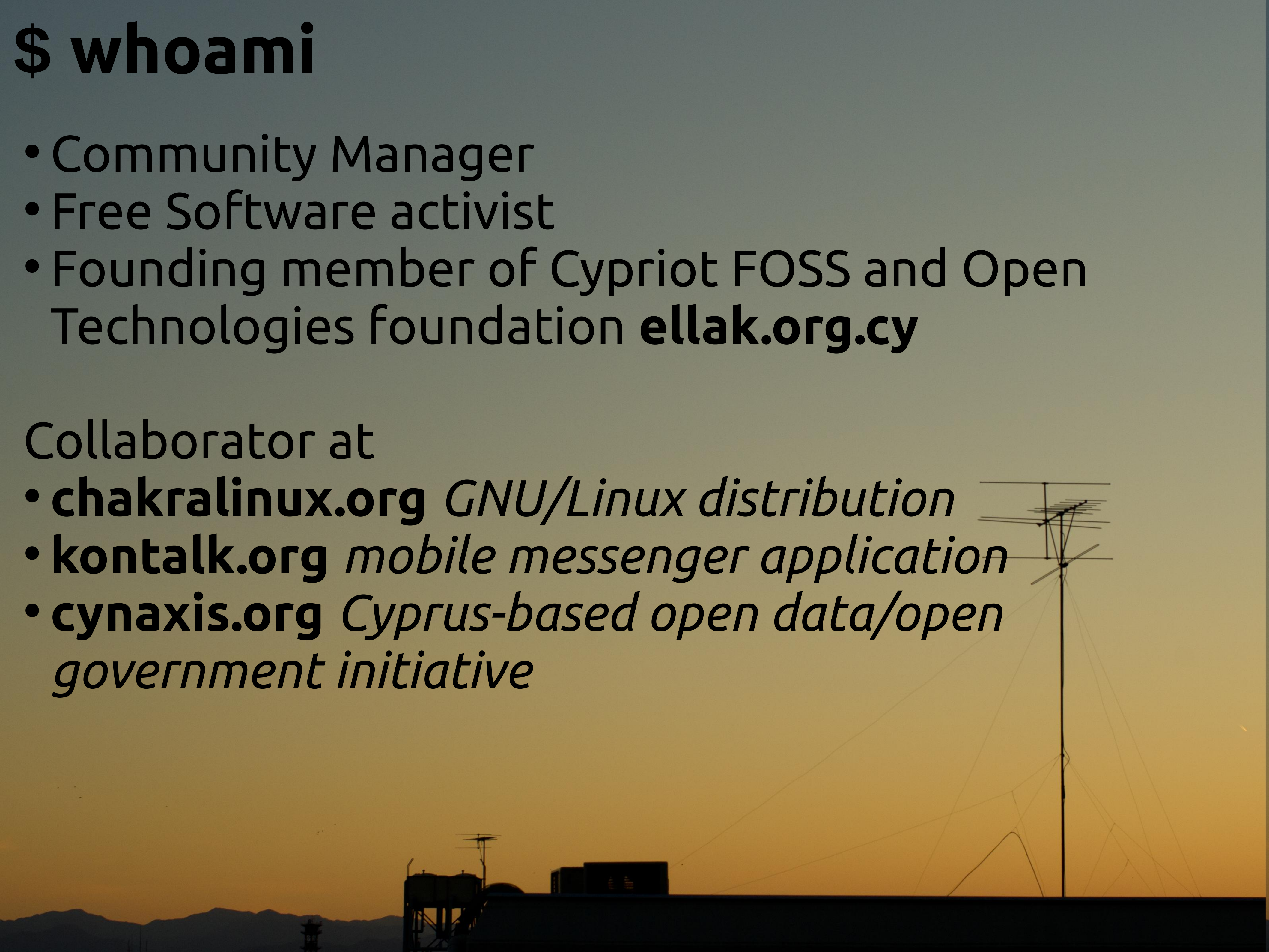
https://www.flickr.com/photos/sudhee/82891943/

$ whoami

- Community Manager
- Free Software activist
- Founding member of Cypriot FOSS and Open Technologies foundation **ellak.org.cy**

Collaborator at

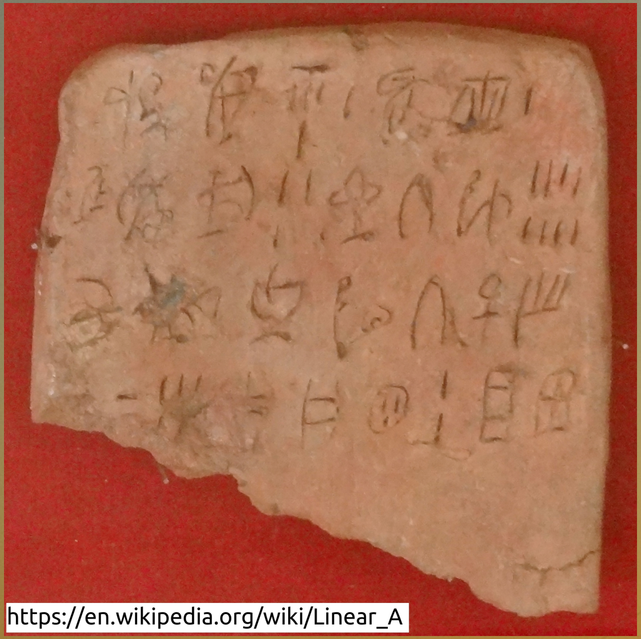
- **chakralinux.org** *GNU/Linux distribution*
- **kontalk.org** *mobile messenger application*
- **cynaxis.org** *Cyprus-based open data/open government initiative*



$ whoiamnot

Disclaimer

- **IANAC** I Am Not A Coder
- Any mistakes or omissions are unintentional



https://en.wikipedia.org/wiki/Linear_A

The new standard

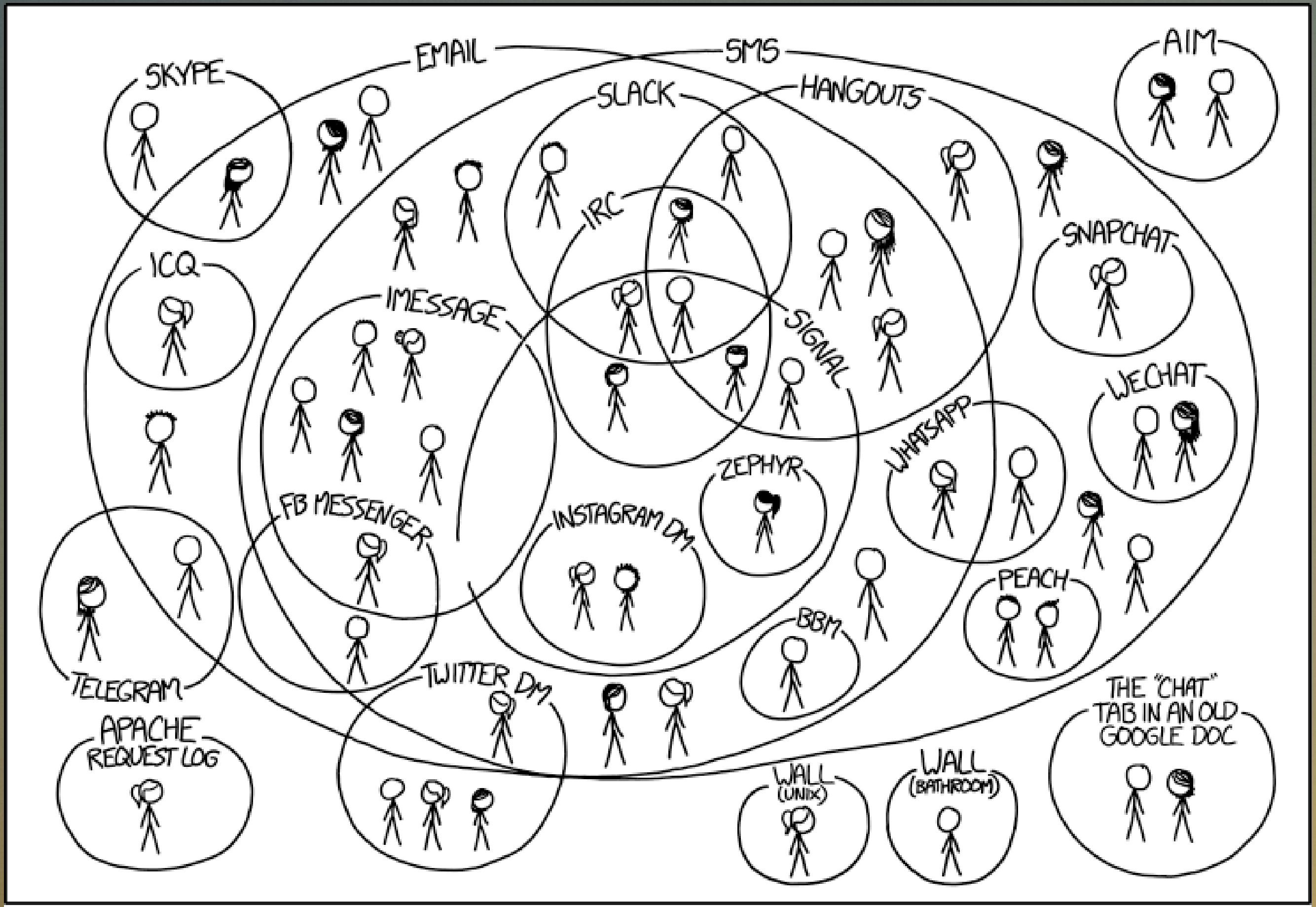
Internet based mobile messenger applications

Traditional text messages and phone calls

Internet based communications

- Free of charge
- Text Messaging
- Group chats
- Audio and Video calls

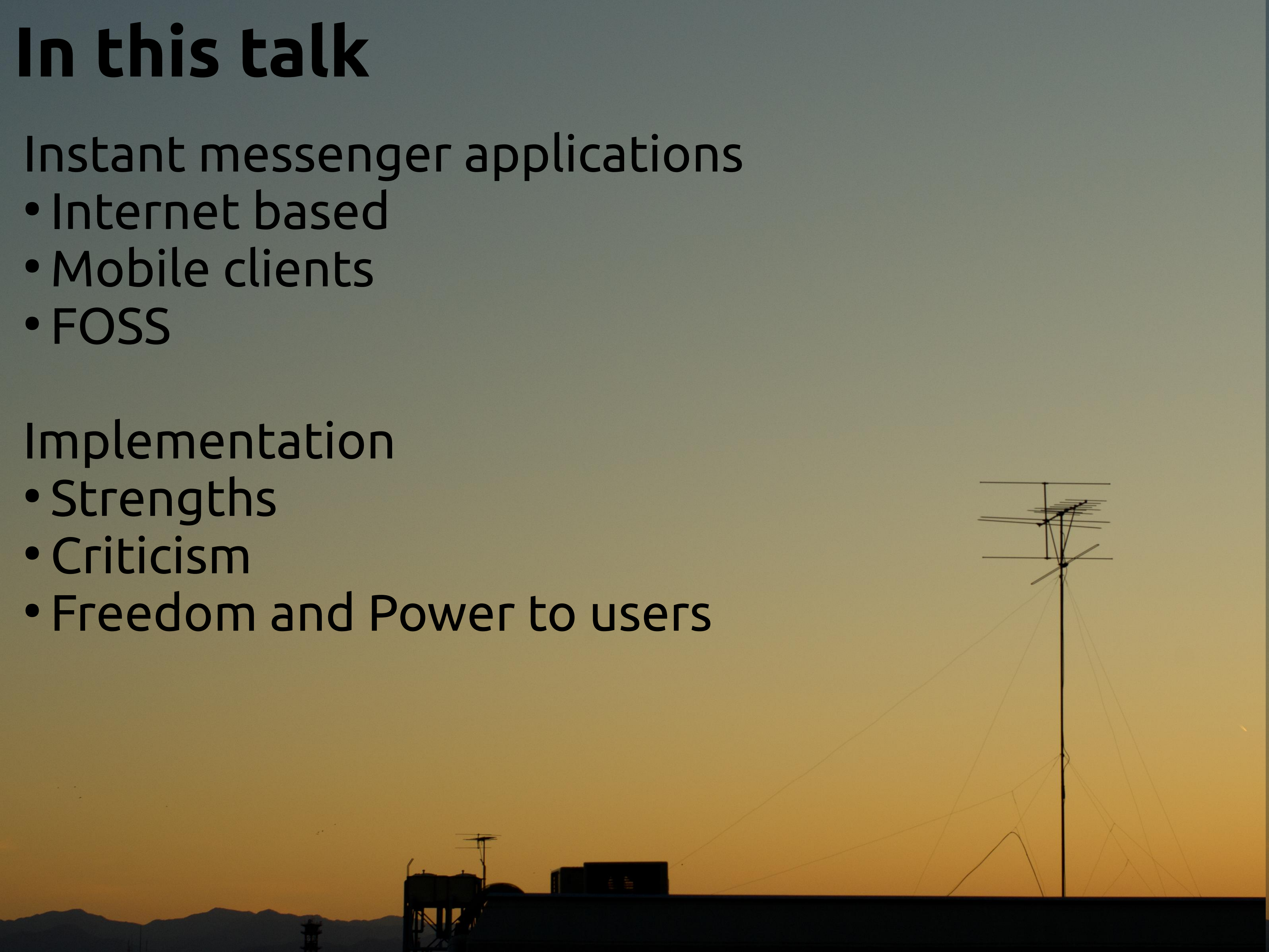
How many apps do you use?



I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.

https://xkcd.com/1810/

In this talk



Instant messenger applications

- Internet based
- Mobile clients
- FOSS

Implementation

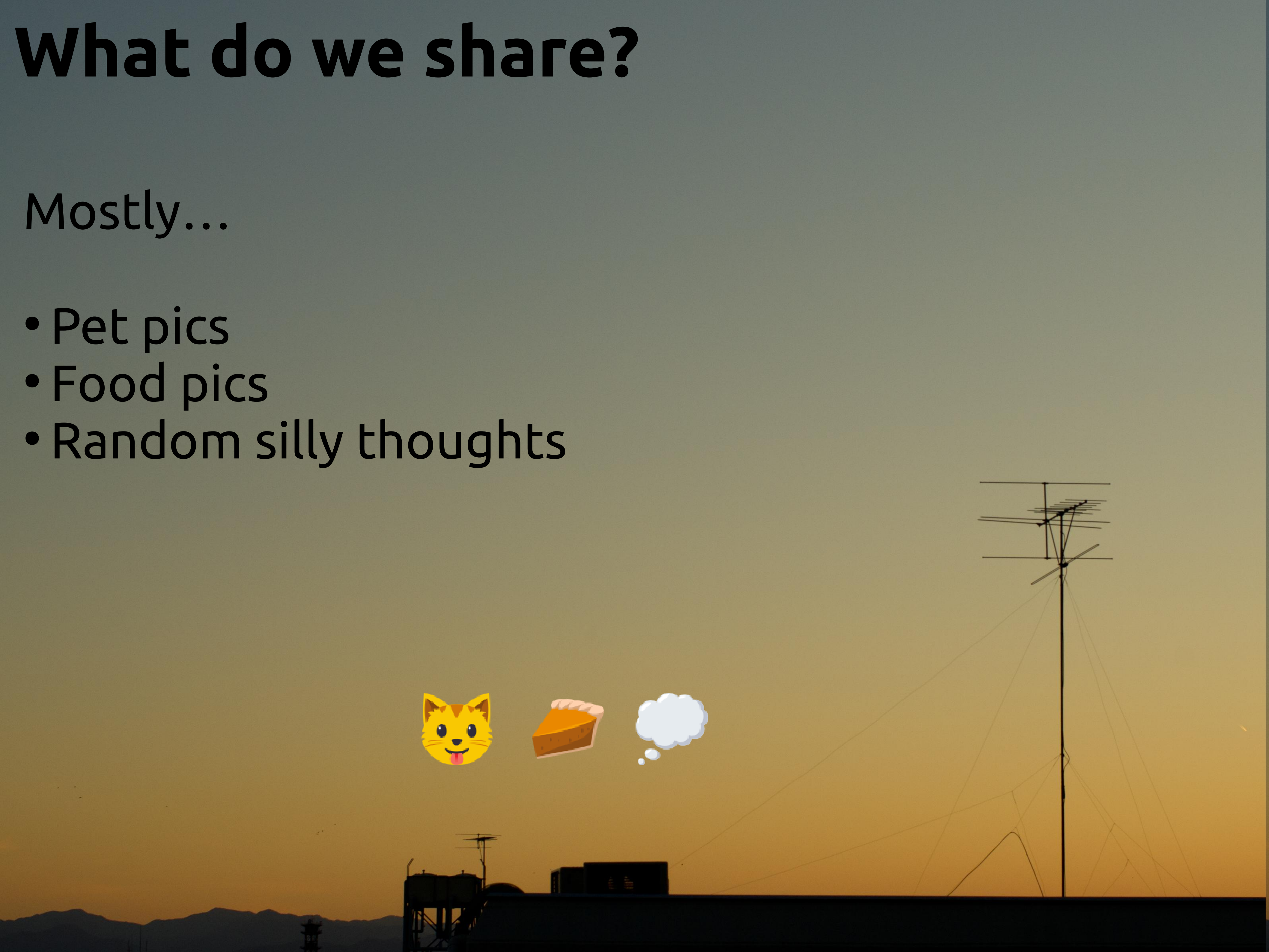
- Strengths
- Criticism
- Freedom and Power to users

What do we share?

Mostly…

- Pet pics
- Food pics
- Random silly thoughts

🐱 🥧 💭



What do we share?

Don't forget…

- Private thoughts
- Personal photos
- Beliefs
- Secrets
- Personal details

🤫 👨‍👧‍👦 👳 🤐 🤕

What is Privacy?

Privacy

- Be secluded from others
- Choose what to share with others

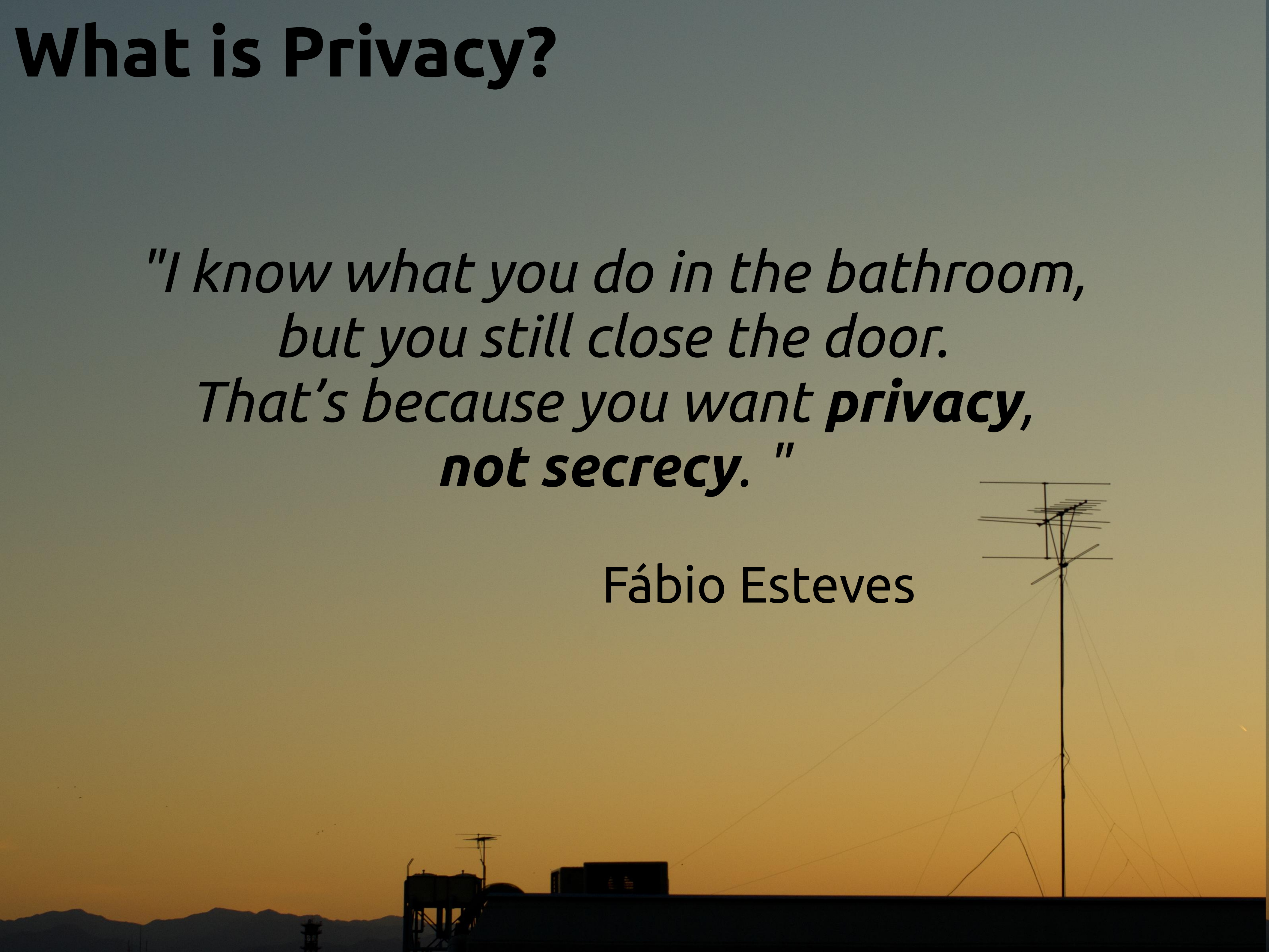
Secrecy

- Keeping information hidden

Anonymity

- Identity concealed

What is Privacy?



"I know what you do in the bathroom,
but you still close the door.
That’s because you want ***privacy****,*
not secrecy*. "*

Fábio Esteves

Privacy in communications

Internet and Digital era

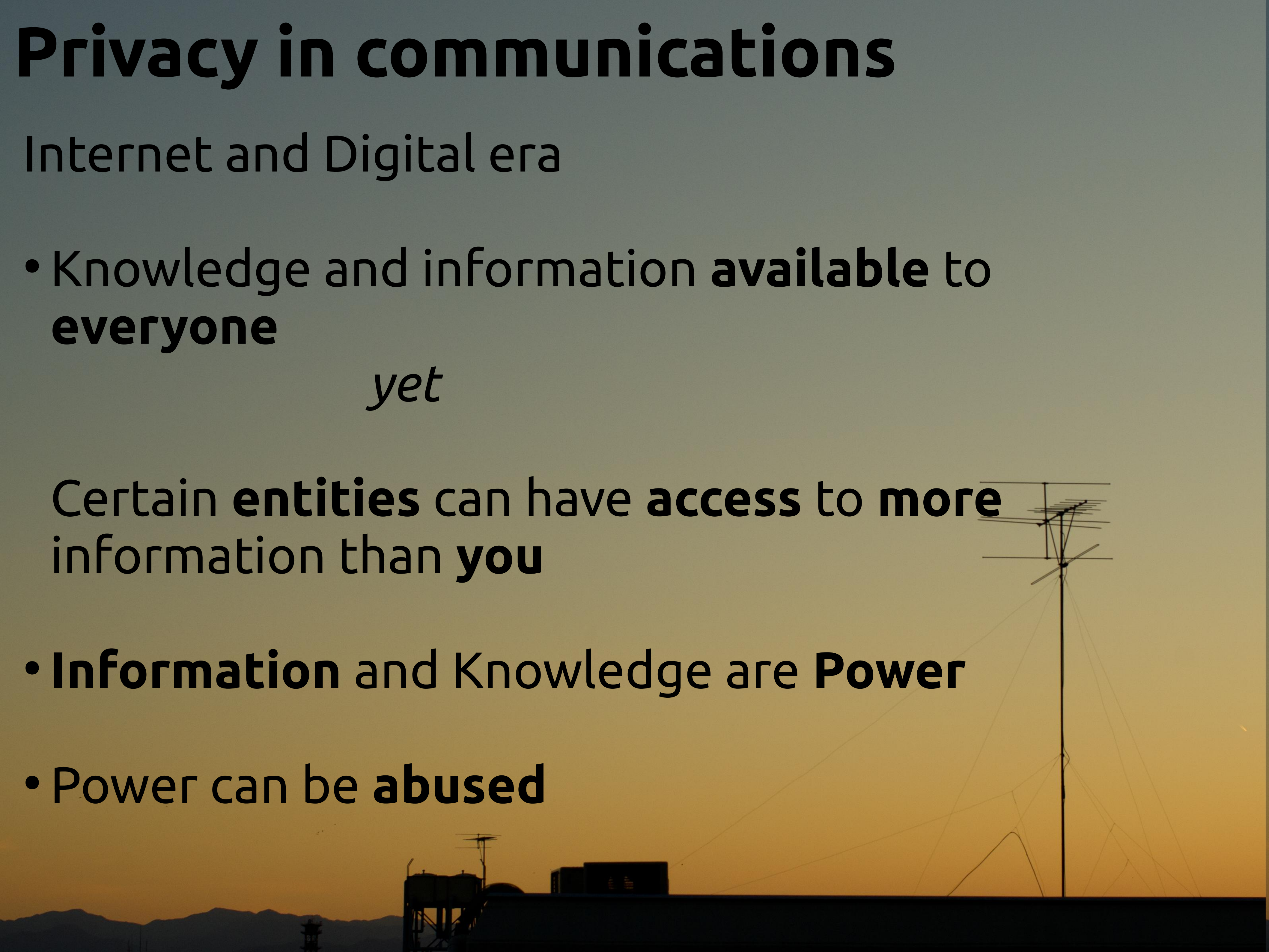
- Knowledge and information **available** to **everyone**

  yet

  Certain **entities** can have **access** to **more** information than **you**

- **Information** and Knowledge are **Power**

- Power can be **abused**



Privacy in communications

Collected communication data is a powerful weapon in the wrong hands

- **Governments** abusing their power
- Authoritarian **regimes**
- Companies **monetizing** personal data

Privacy in communications

Implications of collecting communication data

- **Personal:** Surveillance > Affects behavior
- **Social:** Free Speech and Activism > Suppression
- **Political:**
  Opinions > Manipulation
  Politicians > Influence
- **Financial:** Ideas and Secrets > Stealing

Being FOSS *The essential first step*

Insist on FOSS in communication applications

- **Audit** by anyone at any time
- **Verification** of functionality
- **Transparency** builds trust
- **Self-Hosted** if needed

FREE SOFTWARE.

FREE SOCIETY.

FSF.ORG

Being FOSS *Not enough on its own*

Additional concerns

- Server **implementation**
- Service and privacy **policies**
- Storing of data and **metadata**
- **Compatibility** and **interoperability**
- Closed platforms and **walled gardens**
- **Censorship** and **denial of service**

Being FOSS *Not enough on its own*

To the rescue

- Encryption
- Federation
- Decentralization

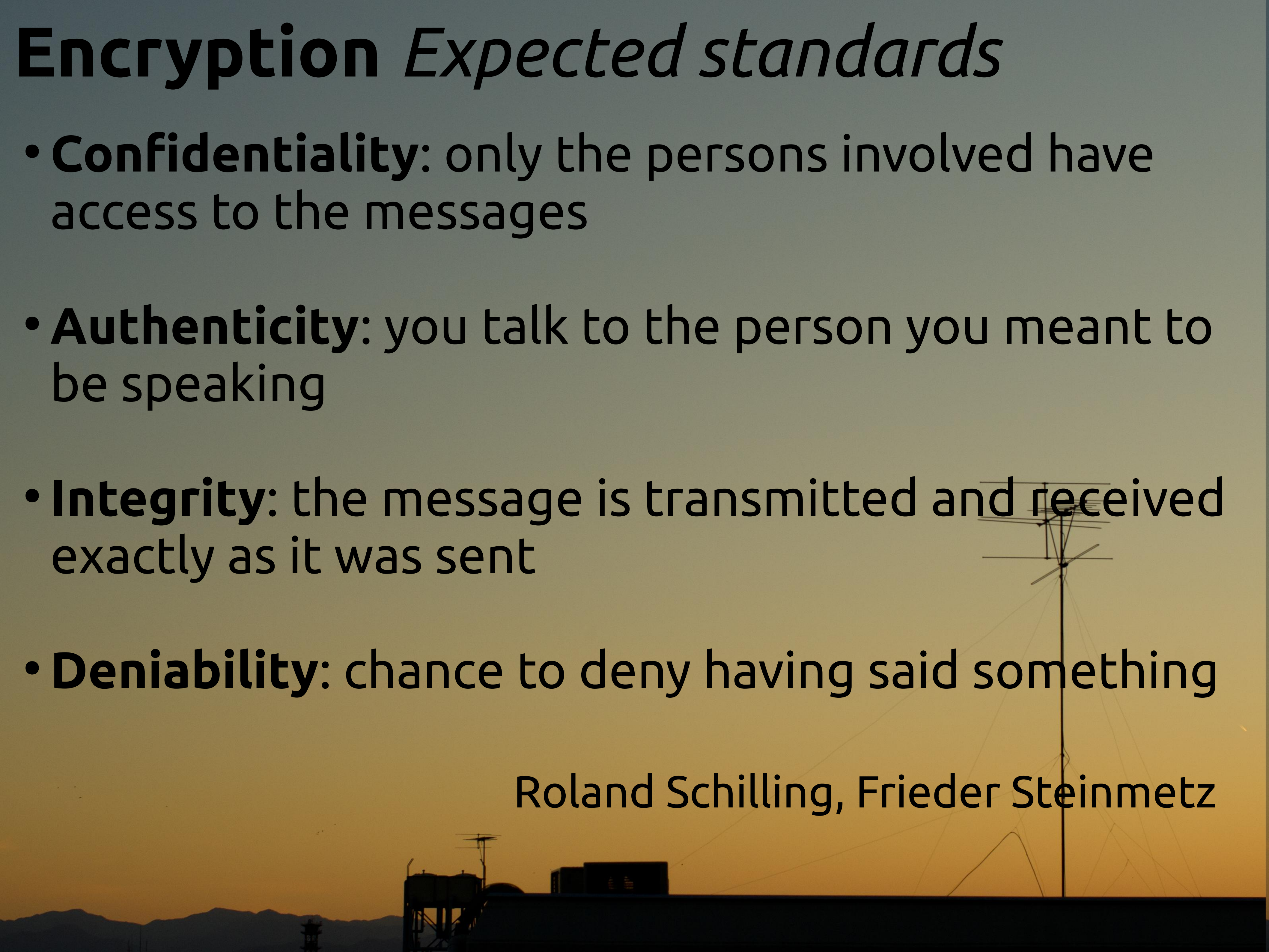
Encryption

"The process of **encoding** a message or **information** in such a way that only **authorized** parties can **access** it."

Wikipedia

https://www.flickr.com/photos/ideonexus/5175383269

Encryption *Expected standards*



- **Confidentiality**: only the persons involved have access to the messages
- **Authenticity**: you talk to the person you meant to be speaking
- **Integrity**: the message is transmitted and received exactly as it was sent
- **Deniability**: chance to deny having said something

Roland Schilling, Frieder Steinmetz

Encryption *end-to-end*

Messages cannot be read by providers of:

- internet service
- communication service
- application software

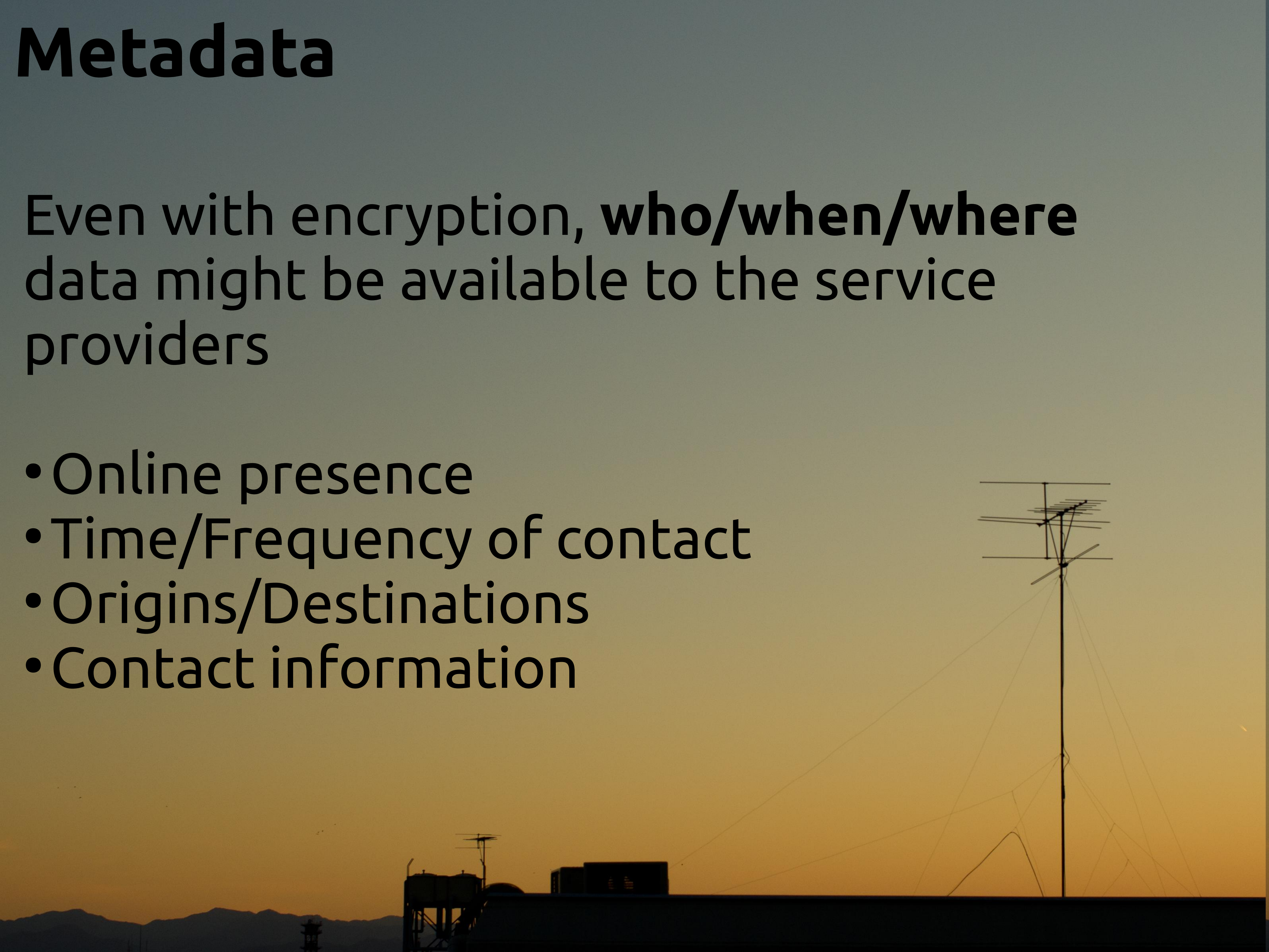
Encryption *Implementation*

- **Perfect forward secrecy**
"a property of secure communication protocols in which compromise of long-term keys does not compromise past session keys" Wikipedia

- **Widely accepted methodologies**
Do not roll your own

- **FOSS**

- **Simple** to use

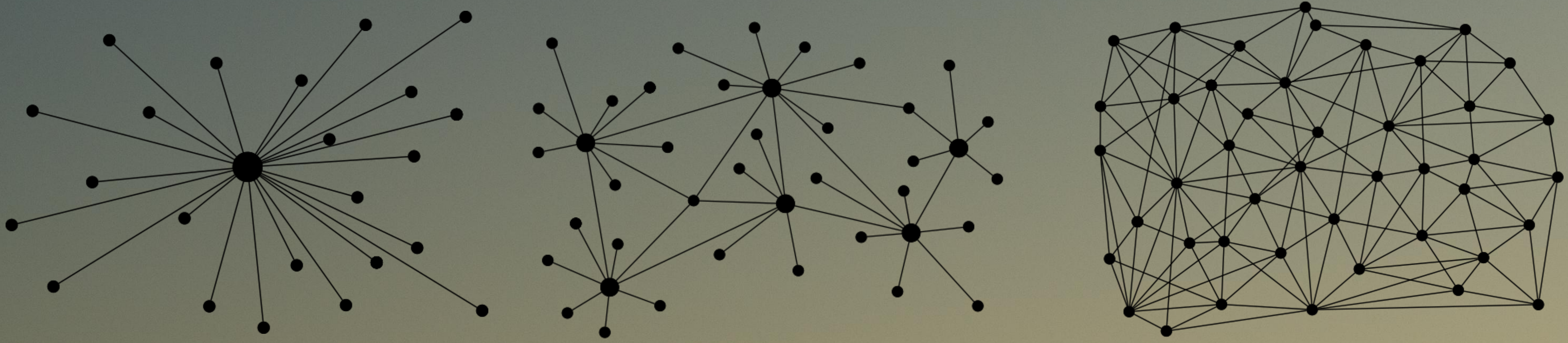


Metadata

Even with encryption, **who/when/where** data might be available to the service providers

- Online presence
- Time/Frequency of contact
- Origins/Destinations
- Contact information

Network Architectures

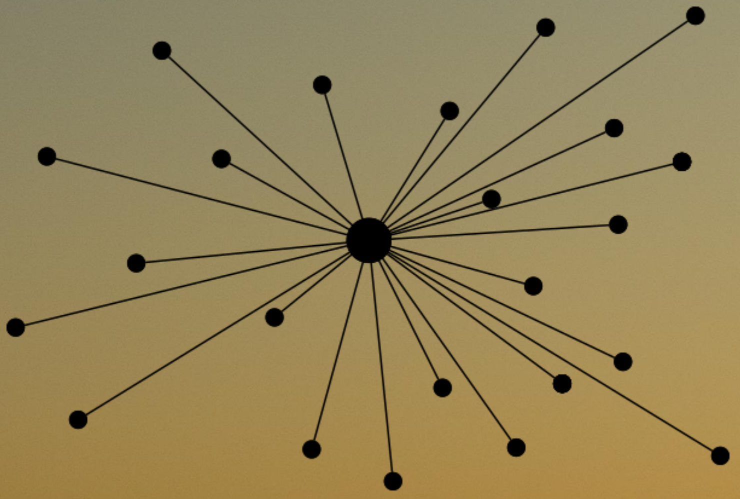


Centralized Federated Decentralized

https://blog.grobox.de/2016/briar-next-step-of-the-crypto-messenger-evolution/

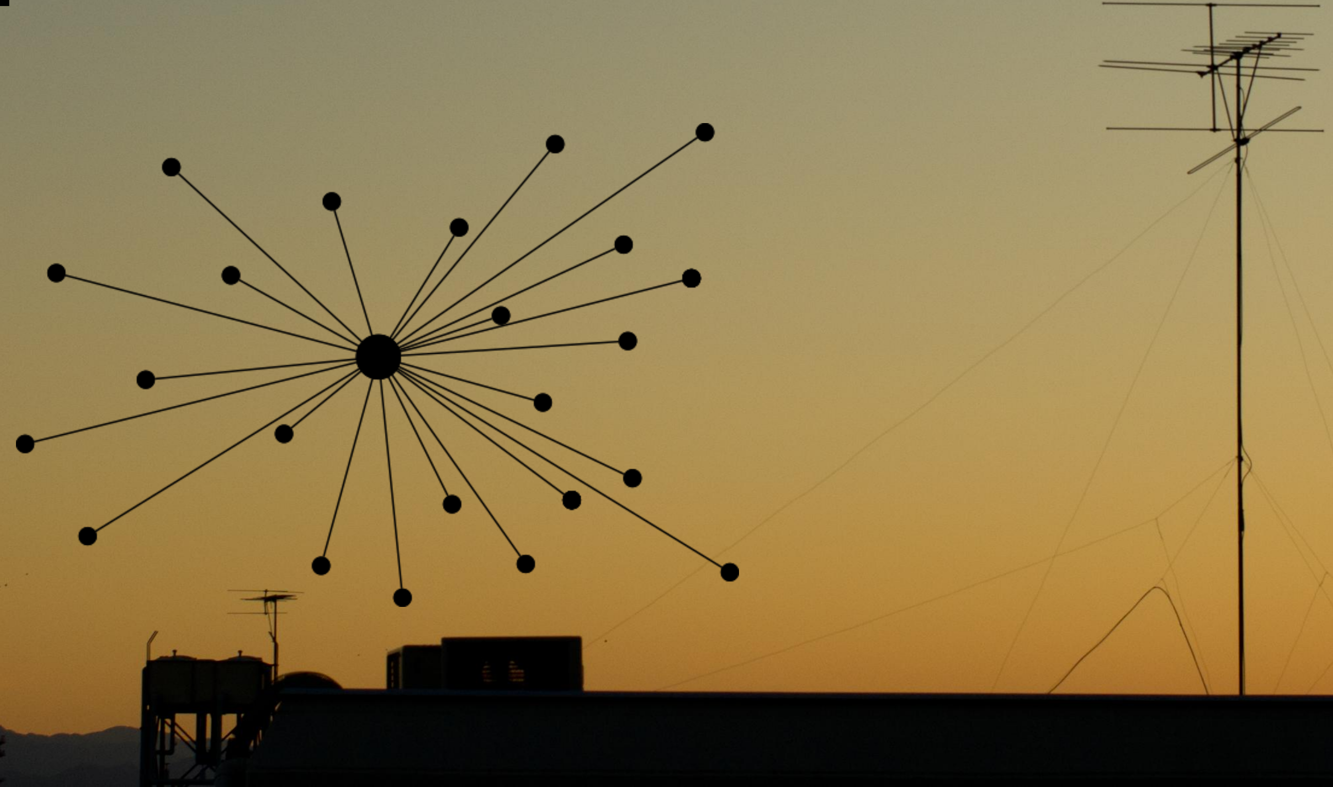
Centralized Services *Advantages*

- Provider has **full authority**
- **Quicker** deployment of new features and changes
- Brand and **quality control**



Centralized Services *Disadvantages*

- **All data** under one entity
- **Metadata** stored
- **Enforcement** of changes (antifeatures)
- **Closed platforms** and **walled gardens**
- **Censorship** and **denial of service**

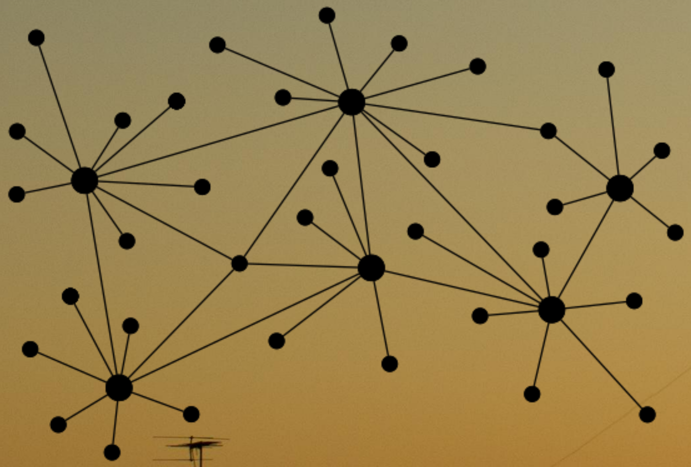


Federation

The ability of independent instances of a service to communicate with each other

Full federation is **independent** of clients and providers

examples: email, sms

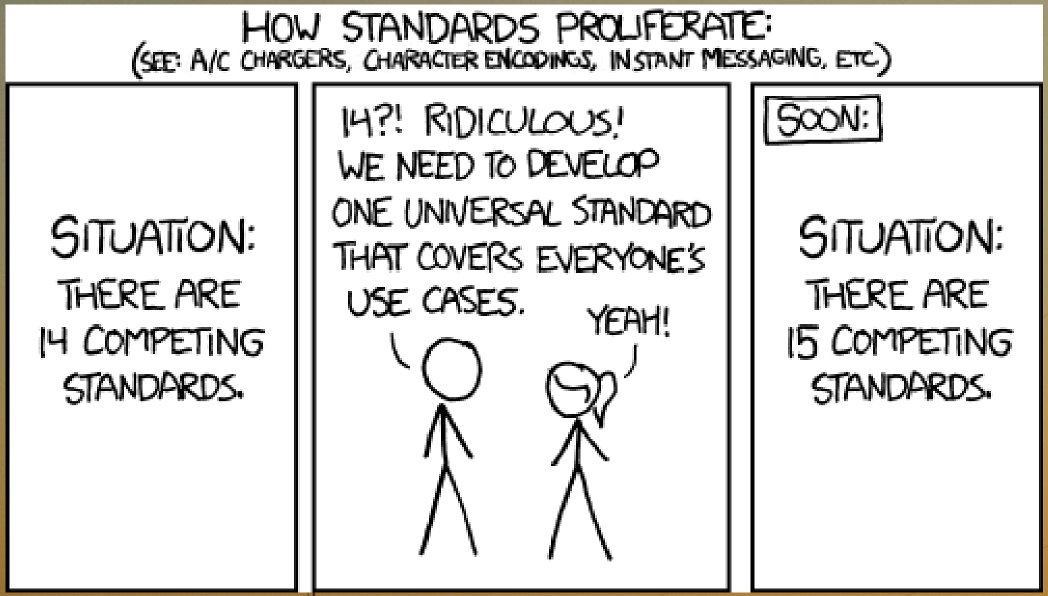


Federation *Advantages*

- Setup and run **individual servers**
- **Choice** among providers
- Difficult to be **denied access** to a service
- Difficult to **bring down** the whole network
- **Data spread** across multiple instances

Federation *Disadvantages*

- **Inconsistent** versions and features among providers (possible advantage?)
- Still a server-client model
- Extremely difficult to reach agreement on **common standards**


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Decentralization

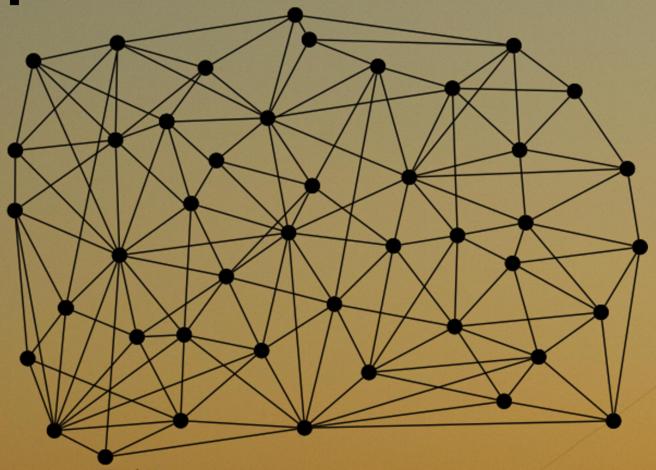
"the process of distributing or dispersing functions, powers, people or things away from a central location or authority"

Wikipedia

examples: peer to peer technologies

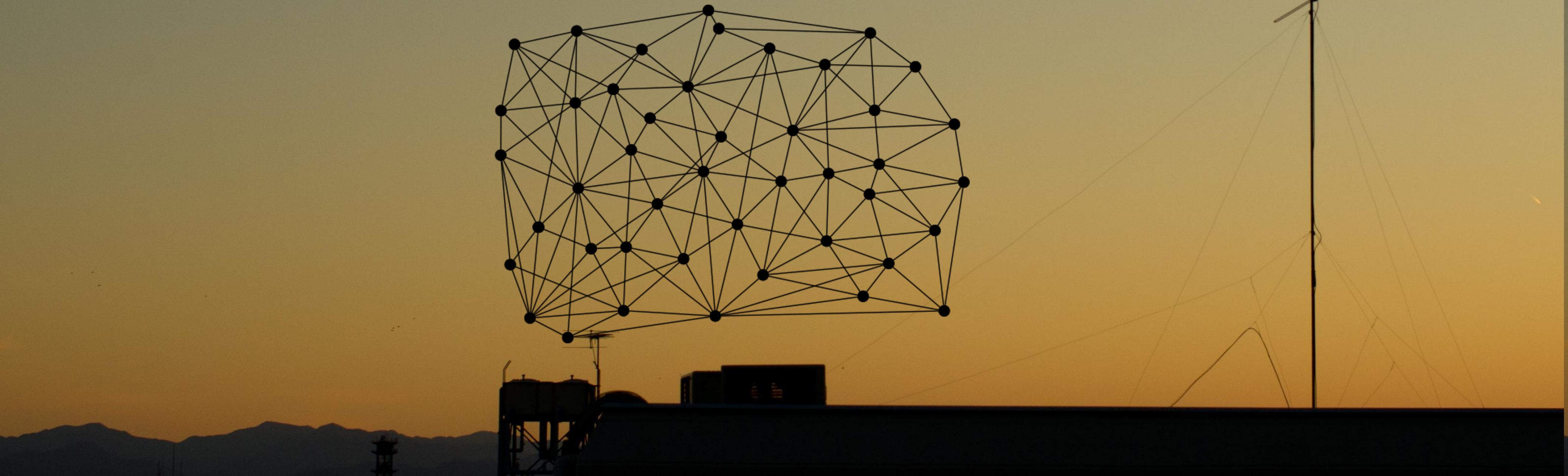
Decentralized Services *Advantages*

- **No dependency** on central provider
  - > server-client model obsolete
- **Resistant to**
  - ✗ Censorship
  - ✗ Denial of Service
  - ✗ Malfunction
  - ✗ Attacks

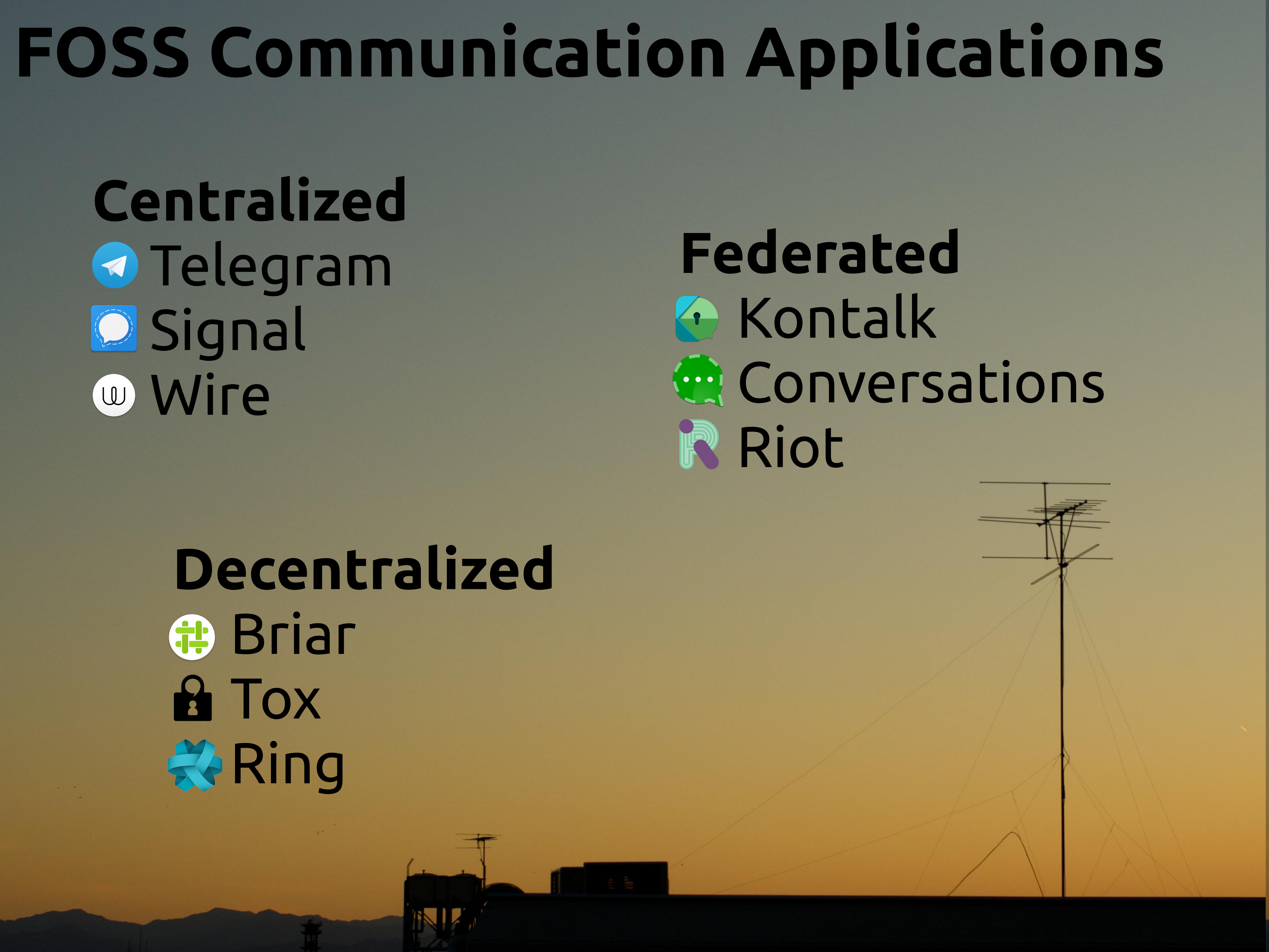


Decentralized Services *Disadvantages*

- **Demanding** on **resources**
  - bandwidth usage and battery drain
  - high number of connections to maintain
- **No offline** messaging
- **No** automatic **contact discovery**
- Available applications still **in development**



FOSS Communication Applications



Centralized

- Telegram
- Signal
- Wire

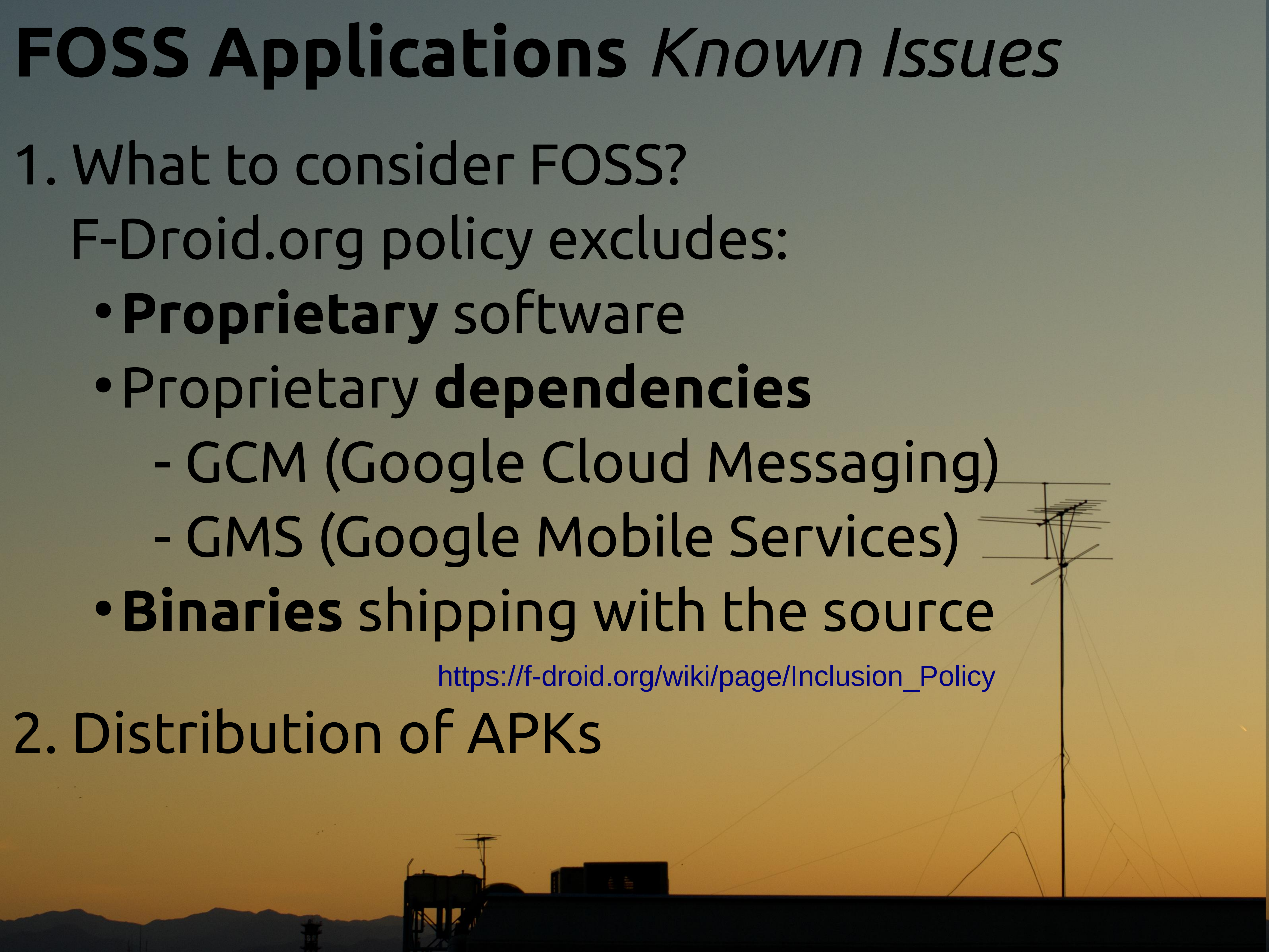
Federated

- Kontalk
- Conversations
- Riot

Decentralized

- Briar
- Tox
- Ring

FOSS Applications *Known Issues*



1. What to consider FOSS?

   F-Droid.org policy excludes:

   - **Proprietary** software
   - Proprietary **dependencies**

     - GCM (Google Cloud Messaging)

     - GMS (Google Mobile Services)
   - **Binaries** shipping with the source

   https://f-droid.org/wiki/page/Inclusion_Policy

2. Distribution of APKs

FOSS Communication Applications

The good news:

Google is considering moving Play Services/GMS libraries under the new **Firebase** name and **open sourcing** them

Hans-Christoph Steiner (F-Droid developer)
https://forum.f-droid.org/t/monthly-development-reports/166/13

Centralized Applications

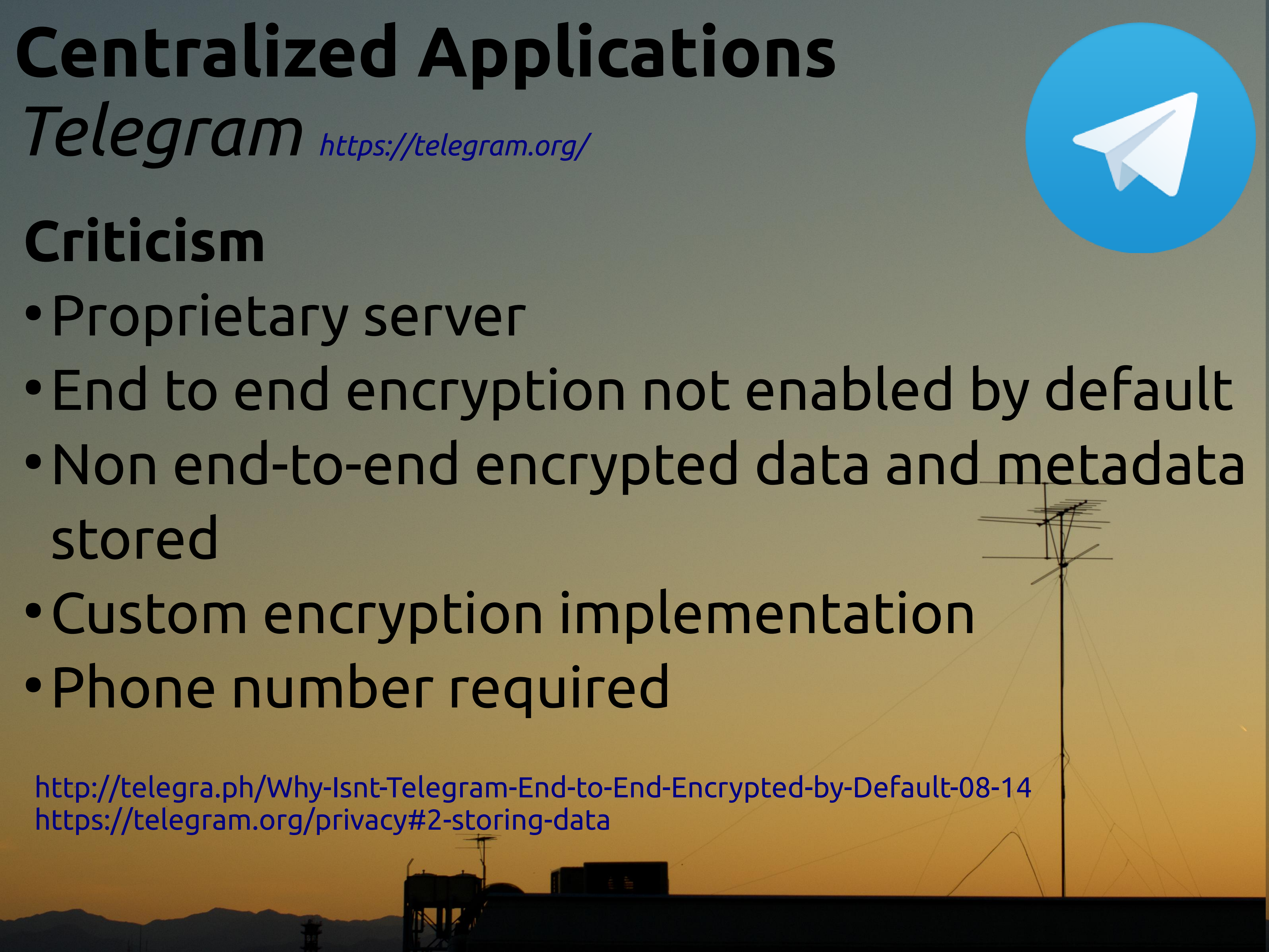
Telegram *https://telegram.org/*

Strengths

- Several FOSS clients (GPLv2, v3)
- End-to-end encryption possible
- Cross platform (synchronization and history)
- Bridges to other services
- High adoption
- Audio calls
- Automatic contact discovery

Centralized Applications

Telegram *https://telegram.org/*



Criticism

- Proprietary server
- End to end encryption not enabled by default
- Non end-to-end encrypted data and metadata stored
- Custom encryption implementation
- Phone number required

http://telegra.ph/Why-Isnt-Telegram-End-to-End-Encrypted-by-Default-08-14
https://telegram.org/privacy#2-storing-data

Centralized Applications

Signal *https://signal.org/*

Strengths

- FOSS client (GPLv3) and server (AGPLv3)
- End-to-end encryption only option
- Widely accepted encryption protocol
- Video and audio calls (peer to peer)
- Combines usability and security
- Automatic contact discovery

https://en.wikipedia.org/wiki/Signal_Protocol#Influence

Centralized Applications

Signal *https://signal.org/*

Criticism

- Metadata stored (some temporarily)
- Communication with self-hosted servers or independently shipped applications blocked
- Phone number required

https://signal.org/signal/privacy/
https://signal.org/blog/the-ecosystem-is-moving/

Centralized Applications

Wire *https://wire.com*

Strengths

- Video/audio calls (conference calls)
- End-to-end encryption by default
- Email or phone number to register
- Multi-device synchronization
- Cross-platform
- FOSS client (GPLv3)
- Partially FOSS server (AGPLv3)

https://wire.com/en/security/

Centralized Applications

Wire *https://wire.com*

Criticism

- Google dependencies in Android client
- Server code not fully available
- Self-hosting documentation still pending
- Federation not available (on the roadmap)
- Metadata stored
- Stores in plain text a list of users contacted to enable syncing across devices

https://github.com/wireapp/wire-android/issues/233
https://medium.com/@wireapp/open-sourcing-wire-server-code-ef7866a731d5
https://wire-docs.wire.com/download/Wire+Privacy+Whitepaper.pdf
https://motherboard.vice.com/en_us/article/secure-messaging-app-wire-stores-everyone-youve-ever-contacted-in-plain-text

Federated Applications

Kontalk *https://kontalk.org*

Strengths

- FOSS client and server (GPLv3)
- Federated (XMPP)
- End-to-end encryption by default (OpenPGP over XMPP)
- Automatic contact discovery via phone numbers

Federated Applications

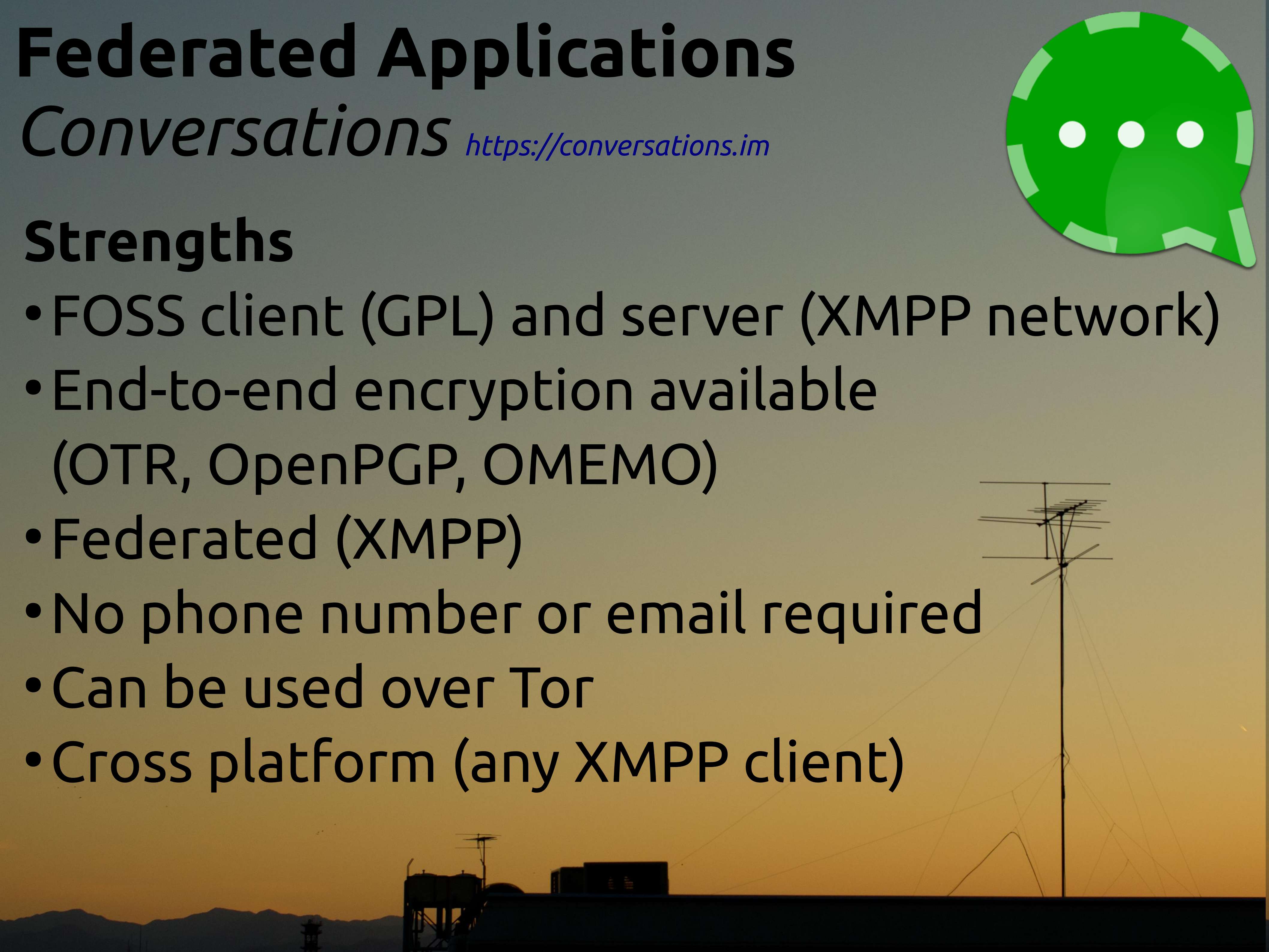
Kontalk *https://kontalk.org*

Criticism

- Phone number required (sha1 hash breakable)
- Encryption
  - No perfect forward secrecy (OMEMO switch planned)
  - Doesn't work outside the Kontalk network
- Metadata stored
- Only one server in the network
- Video/audio calls not supported
- No synchronization among devices
- No iOS client

Federated Applications

Conversations *https://conversations.im*



Strengths

- FOSS client (GPL) and server (XMPP network)
- End-to-end encryption available (OTR, OpenPGP, OMEMO)
- Federated (XMPP)
- No phone number or email required
- Can be used over Tor
- Cross platform (any XMPP client)

Federated Applications

Conversations *https://conversations.im*

Criticism

- Complicated for casual users
  - Zom.im intended to improve this
- End-to-end encryption
  - not enabled by default
  - not available for group chats
- Non end-to-end encrypted data and metadata stored
- Video/audio calls not supported

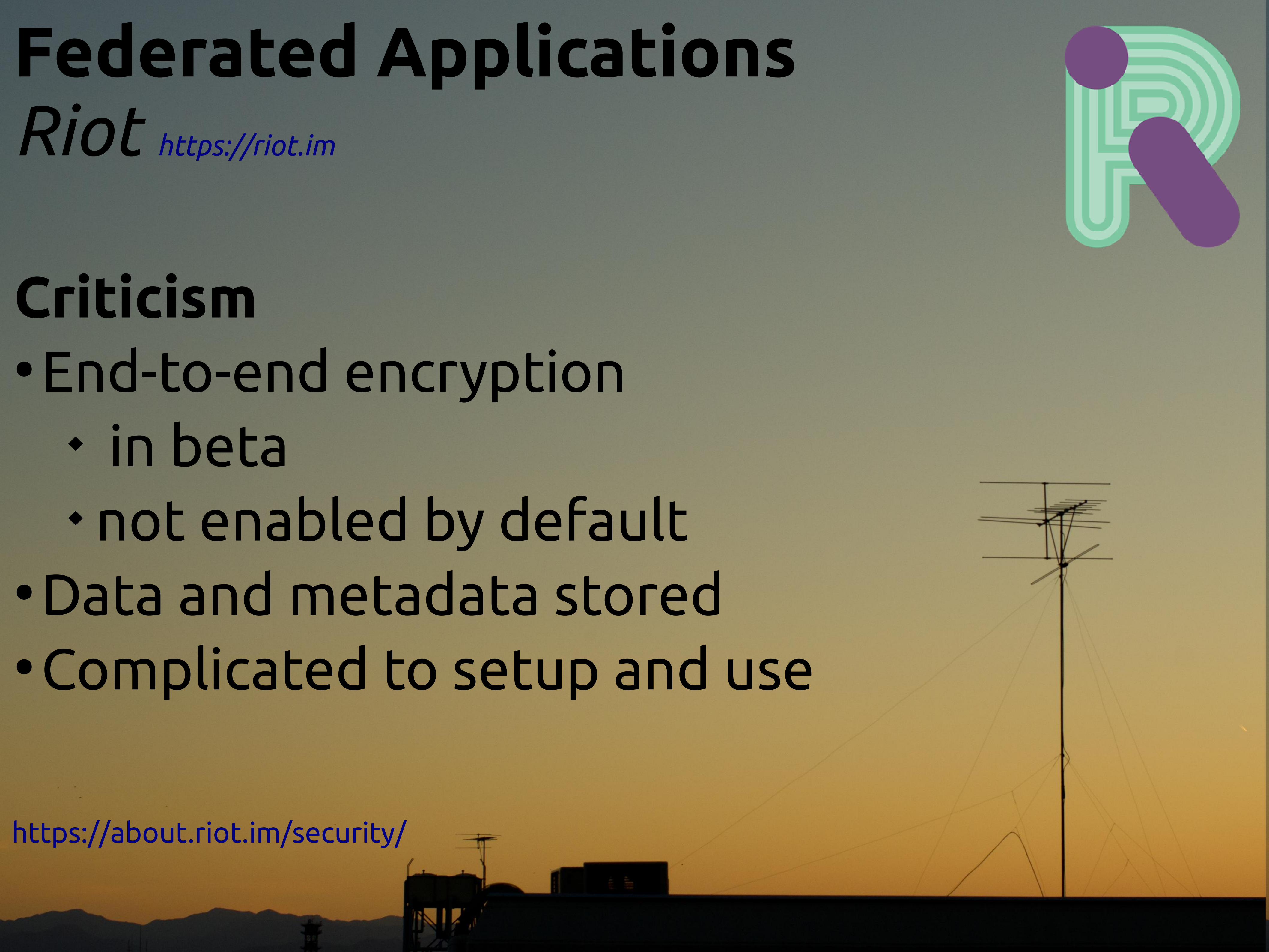
https://chatsecure.org/blog/chatsecure-conversations-zom/

Federated Applications

Riot *https://riot.im*

Strengths

- Completely FOSS (Apache v2)
- Federated (Matrix)
- Bridges for other services
- End-to-end encryption available (implementation of Signal Protocol)
- No phone number or email required
- Cross platform
- Video and audio calls support



Federated Applications

Riot *https://riot.im*

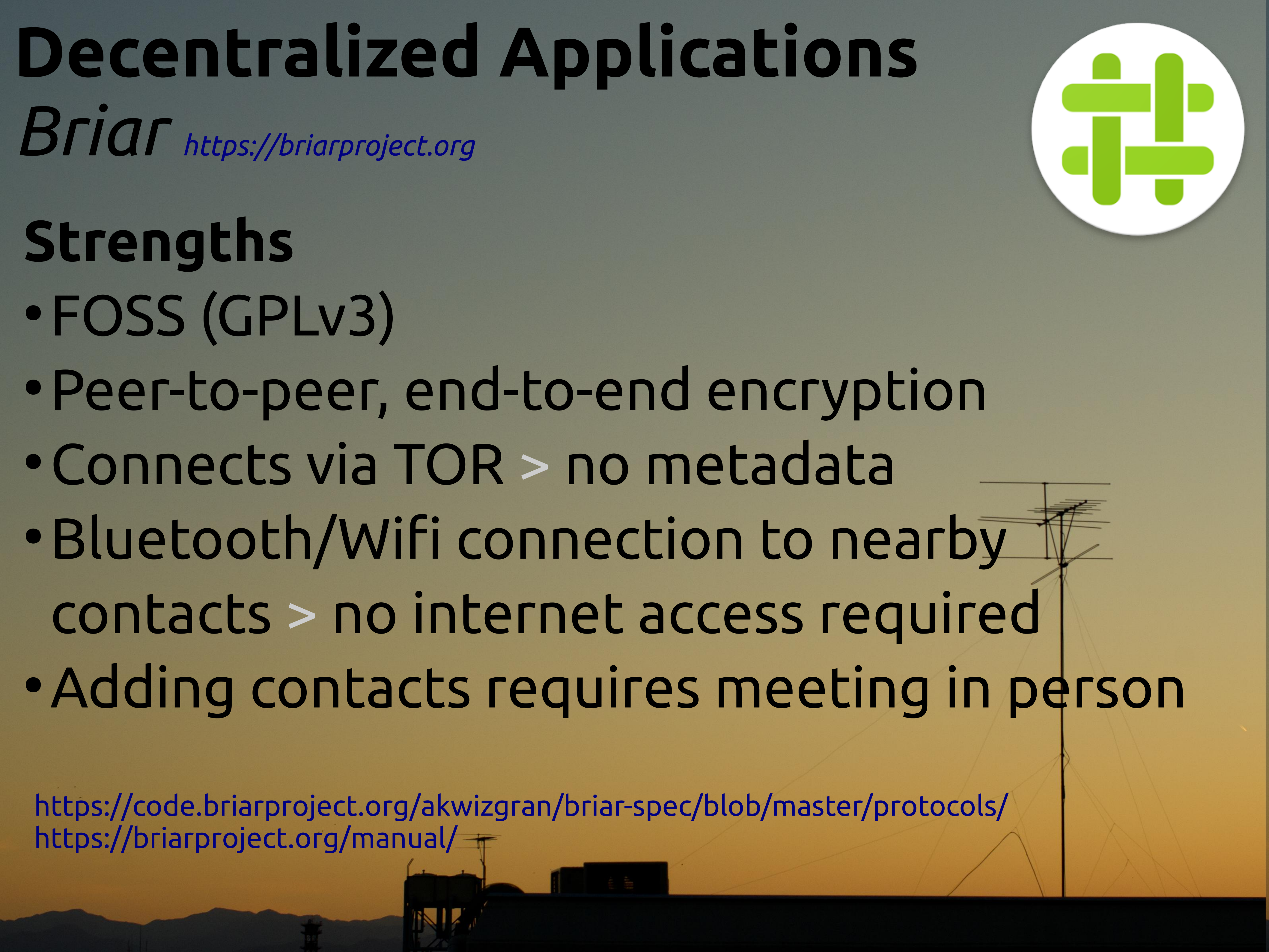
Criticism

- End-to-end encryption
  - in beta
  - not enabled by default
- Data and metadata stored
- Complicated to setup and use

https://about.riot.im/security/

Decentralized Applications

Briar *https://briarproject.org*



Strengths

- FOSS (GPLv3)
- Peer-to-peer, end-to-end encryption
- Connects via TOR > no metadata
- Bluetooth/Wifi connection to nearby contacts > no internet access required
- Adding contacts requires meeting in person

https://code.briarproject.org/akwizgran/briar-spec/blob/master/protocols/
https://briarproject.org/manual/

Decentralized Applications

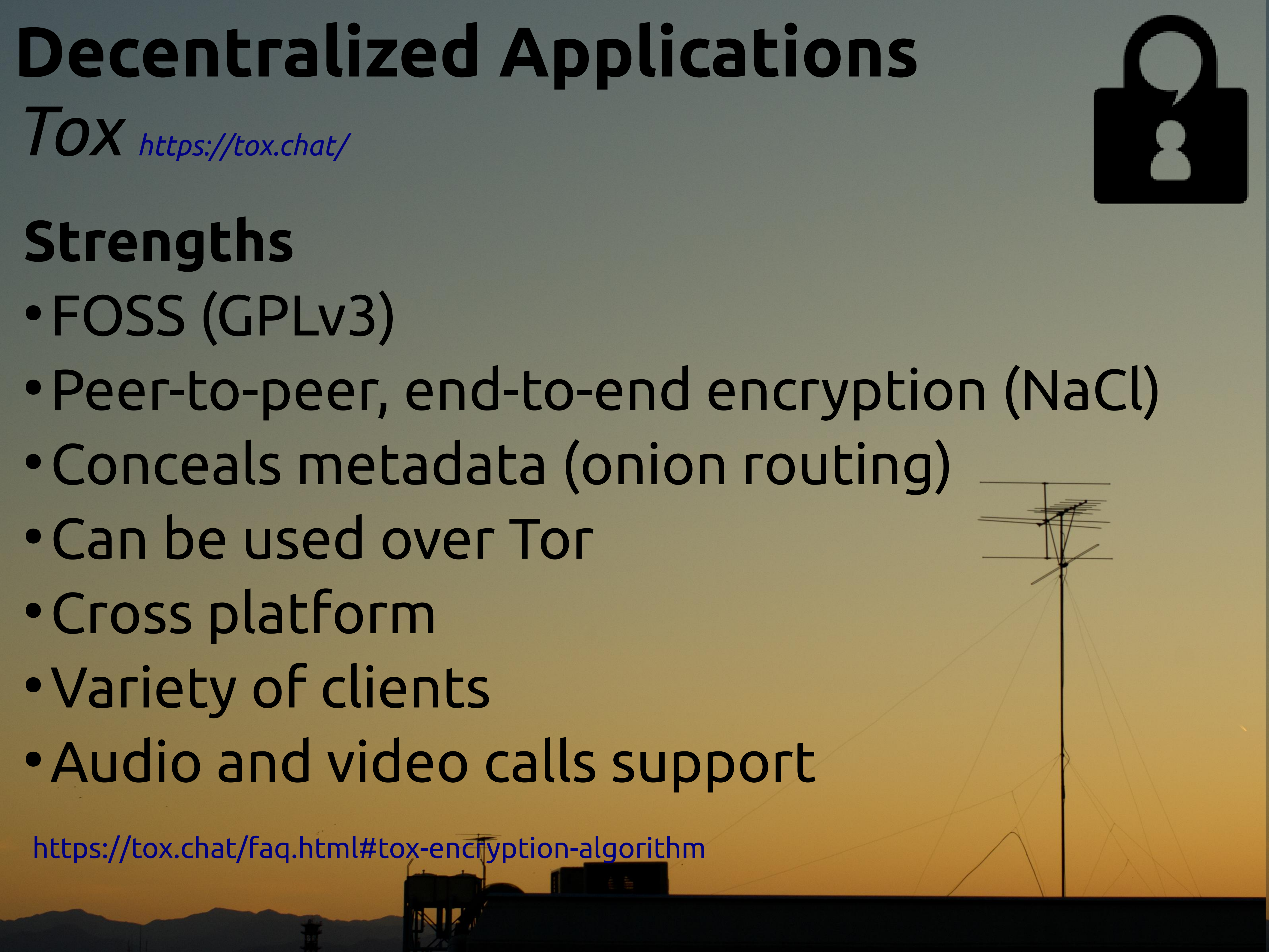
Briar *https://briarproject.org*

Criticism

- No video/audio calls support
- No offline messaging
- Demanding on resources
- Complicated addition of remote contacts
- Only Android client
- Not on F-droid > binary jars
- In development

Decentralized Applications

Tox *https://tox.chat/*



Strengths

- FOSS (GPLv3)
- Peer-to-peer, end-to-end encryption (NaCl)
- Conceals metadata (onion routing)
- Can be used over Tor
- Cross platform
- Variety of clients
- Audio and video calls support

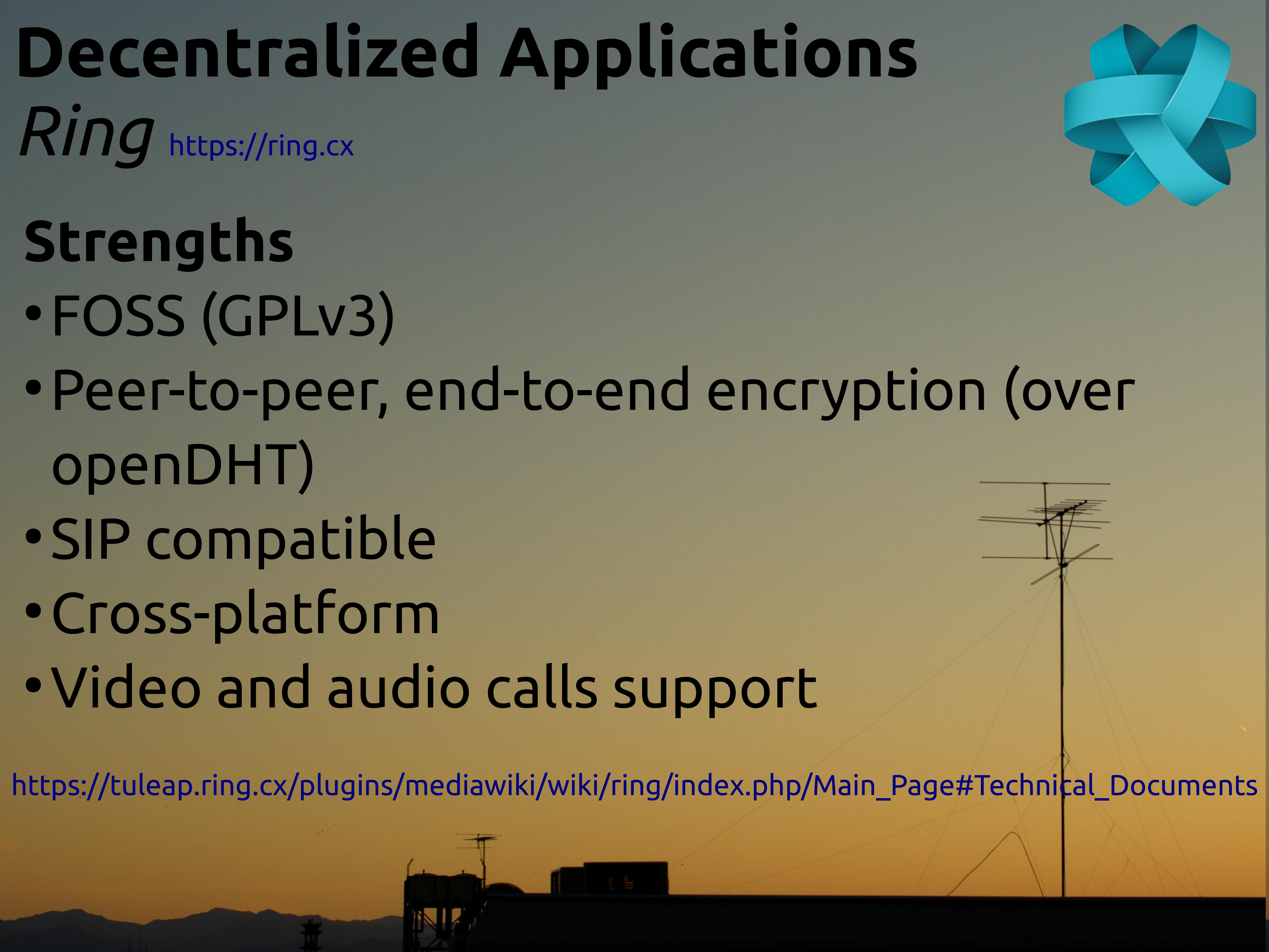
https://tox.chat/faq.html#tox-encryption-algorithm

Decentralized Applications

Tox *https://tox.chat/*

Criticism

- Android clients in development
- Complicated contact discovery > ToxID
- Usability varies depending on the client
- No offline messaging
- Demanding on Resources



Decentralized Applications

Ring https://ring.cx

Strengths

- FOSS (GPLv3)
- Peer-to-peer, end-to-end encryption (over openDHT)
- SIP compatible
- Cross-platform
- Video and audio calls support

https://tuleap.ring.cx/plugins/mediawiki/wiki/ring/index.php/Main_Page#Technical_Documents

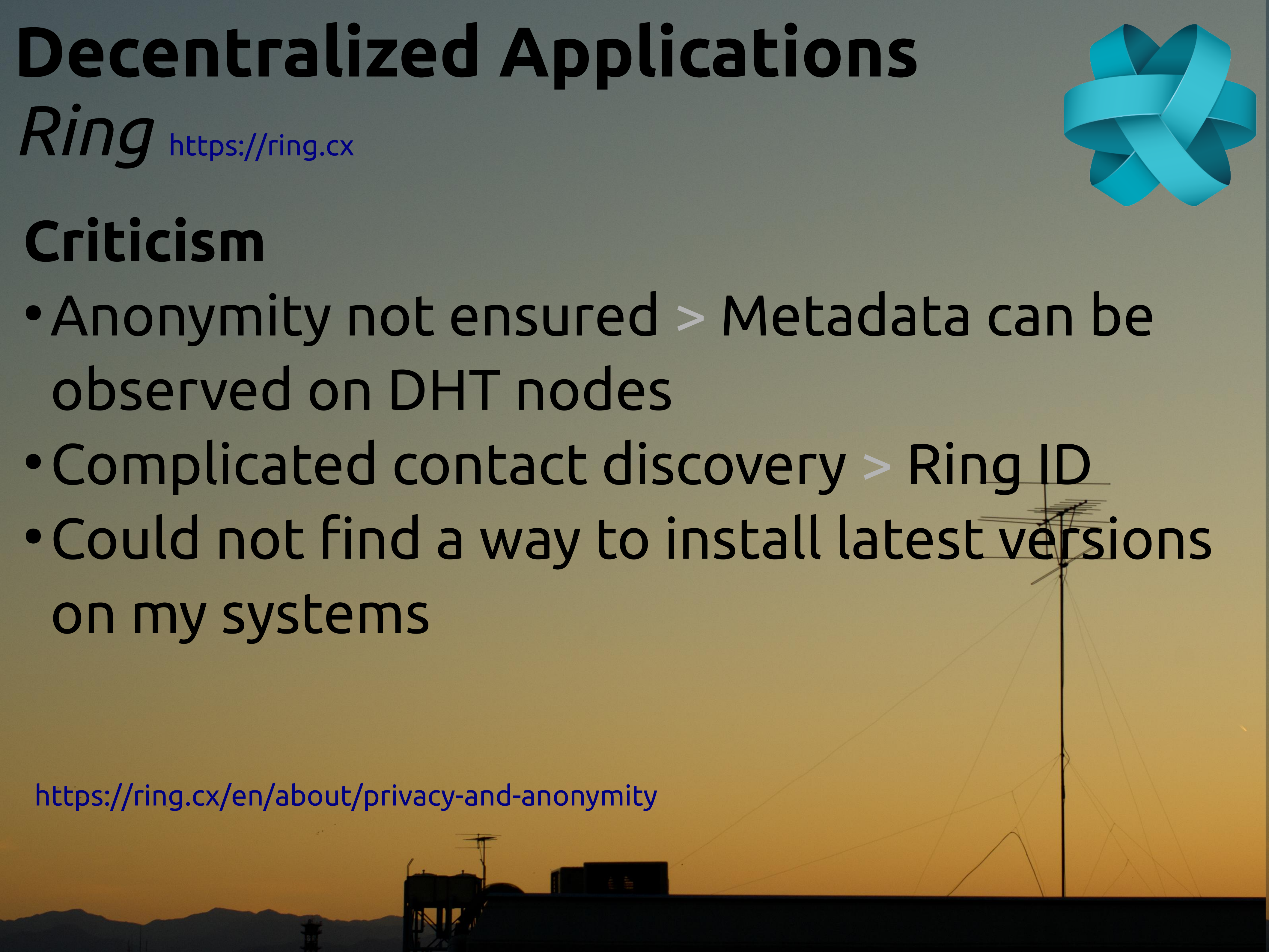
Decentralized Applications

Ring https://ring.cx

Criticism

- Anonymity not ensured > Metadata can be observed on DHT nodes
- Complicated contact discovery > Ring ID
- Could not find a way to install latest versions on my systems

https://ring.cx/en/about/privacy-and-anonymity



Know what you look for

One app to rule them all?

Difficult to **combine:**

- Powerful **encryption** and **simplicity**
- Strong **privacy** and **usability**
- Freedom of **choice** and **centralization**

Know what you look for

Are you…

- a journalist
- an activist
- a whistleblower
- a casual user
- a citizen in an oppressive regime
- a privacy advocate

…?

Know what you look for

We all have different **needs** and **priorities**

✓ FOSS

✓ Privacy

✓ Anonymity

✓ Usability

✓ Federated network

✓ Decentralized Peer to Peer communication

Awareness and Adoption

The biggest problems most apps face

- Do we **care** enough about **privacy**?
- Are we **aware** of our **choices**?
- Are our **contacts available** on their service?

“Privacy is an ecological problem
like second-hand smoking"
Eben Moglen

What can we do?

Advocate

- **Inform** your contacts on the benefits of using privacy respecting applications
- Suggest **suitable** alternatives
- Constructively **voice your concerns** to developers

Contribute to the projects you care about.

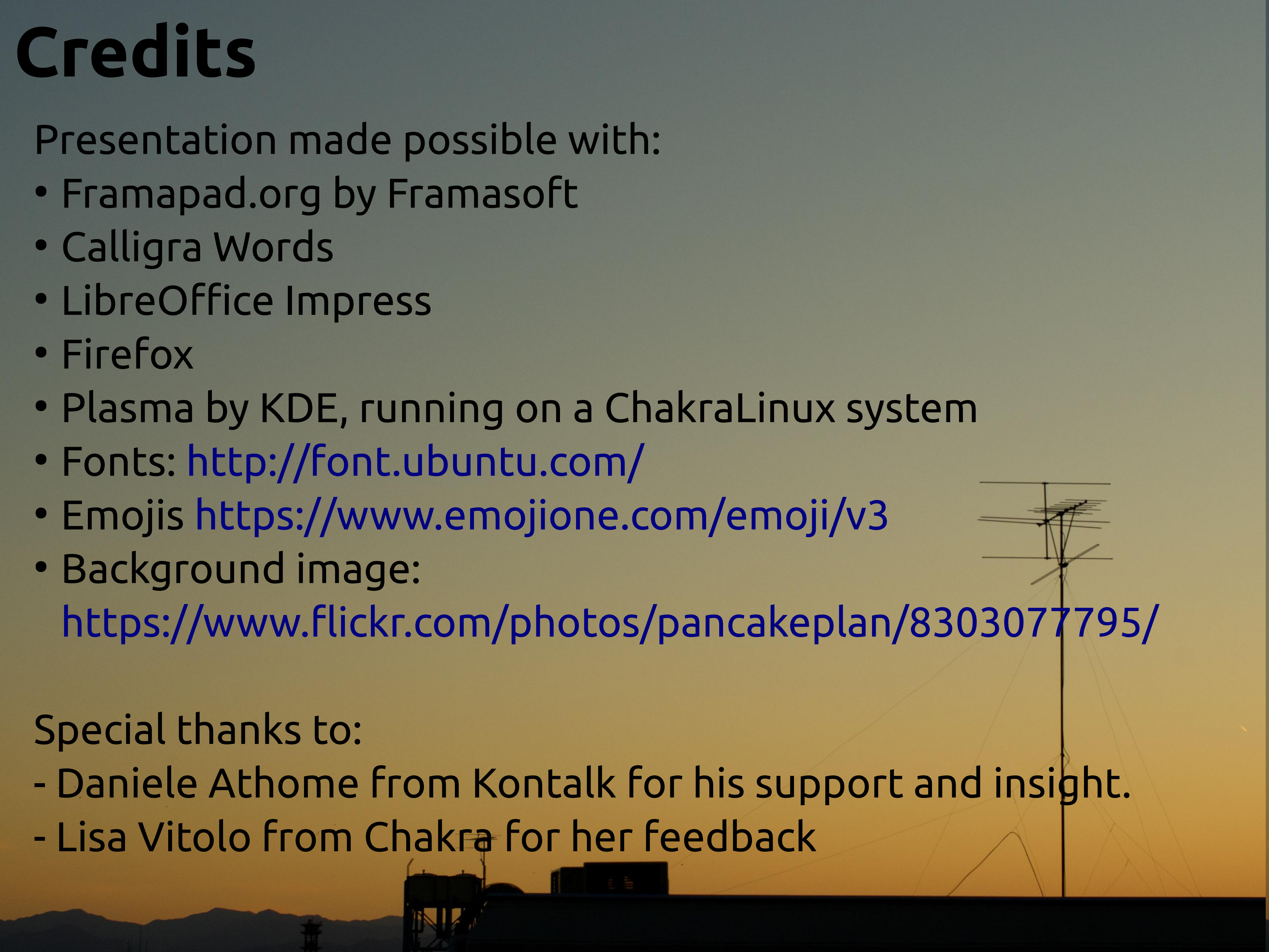
Take home message

- Privacy in communications is **achievable.**
- Quality **FOSS alternatives** to proprietary solutions exist.
- **Encryption**, **federation** and **decentralization** matter.
- Choose an application that matches **your needs.**

References/Further reading

- **EFF** Messaging Scorecard
  https://www.eff.org/secure-messaging-scorecard
- **Hannes Hauswedell** Messenger Table
  https://hannes.hauswedell.net/messenger/
- **Framasoft** De-google-ify Internet
  https://degooglisons-internet.org/
- **Roland Schilling**, **Frieder Steinmetz**: A look into the Mobile Messaging Black Box
  https://fahrplan.events.ccc.de/congress/2016/Fahrplan/events/8062.html
- **Hanno Böck** Are decentralized services unable to innovate?
  https://events.ccc.de/congress/2016/wiki/Session:Are_decentralized_services_unable_to_innovate
- **Michal Wozniak** Free Software and the Network Effect
  https://conf.qtcon.org/en/qtcon/public/events/465.html
- **Eben Moglen, Mishi Choudhary** The last kilometer, the last chance
  https://re-publica.com/en/16/session/opening-keynote-last-kilometer-last-chance
- **Jonas Öberg** Is this the end of decentralizaton?
  http://blog.jonasoberg.net/is-this-the-end-of-decentralisation-2/
- **Fábio Esteves** I have nothing to hide. Why should I care about my privacy?
  https://medium.com/@FabioAEsteves/i-have-nothing-to-hide-why-should-i-care-about-my-privacy-f488281b8f1d
- **Moxie Marlinspike**
  https://signal.org/blog/contact-discovery/
- **Eleanor Saitta** Briar and Bramble: A Vision for Decentralized Infrastructure
  https://dymaxion.org/essays/briarvision.html
- **Torsten Grote** Briar – Next Step of The Crypto Messenger Evolution
  https://blog.grobox.de/2016/briar-next-step-of-the-crypto-messenger-evolution/
- **Privacy Tools**
  https://www.privacytools.io

Credits



Presentation made possible with:

- Framapad.org by Framasoft
- Calligra Words
- LibreOffice Impress
- Firefox
- Plasma by KDE, running on a ChakraLinux system
- Fonts: http://font.ubuntu.com/
- Emojis https://www.emojione.com/emoji/v3
- Background image: https://www.flickr.com/photos/pancakeplan/8303077795/

Special thanks to:

- Daniele Athome from Kontalk for his support and insight.
- Lisa Vitolo from Chakra for her feedback

Questions?

Thank you!

Neofytos Kolokotronis
https://about.me/neofytosk