GNUNET + PSYC = \oXoXo/

WE USED TO FEDERATE

decentralized internet:
everyone has servers
servers federate
no single company

which server to choose & trust?
ccc? brokep? autistici?
gmail+ hotmail+

… even if *your* box is at home

YOUR PERSONAL PRISM NODE

my own server for 8€ a month:

vulnerable cryptography
memory can be monitored
controlling system accessible by observers
automated monitoring of federated networks

… even if *your* box is at home

DO NOT DEPEND ON SERVERS

encrypt end-to-end
forward secrecy
protect connection meta-data
(who? when? how much?)

with GADS & *multicast*
=: GNUnet

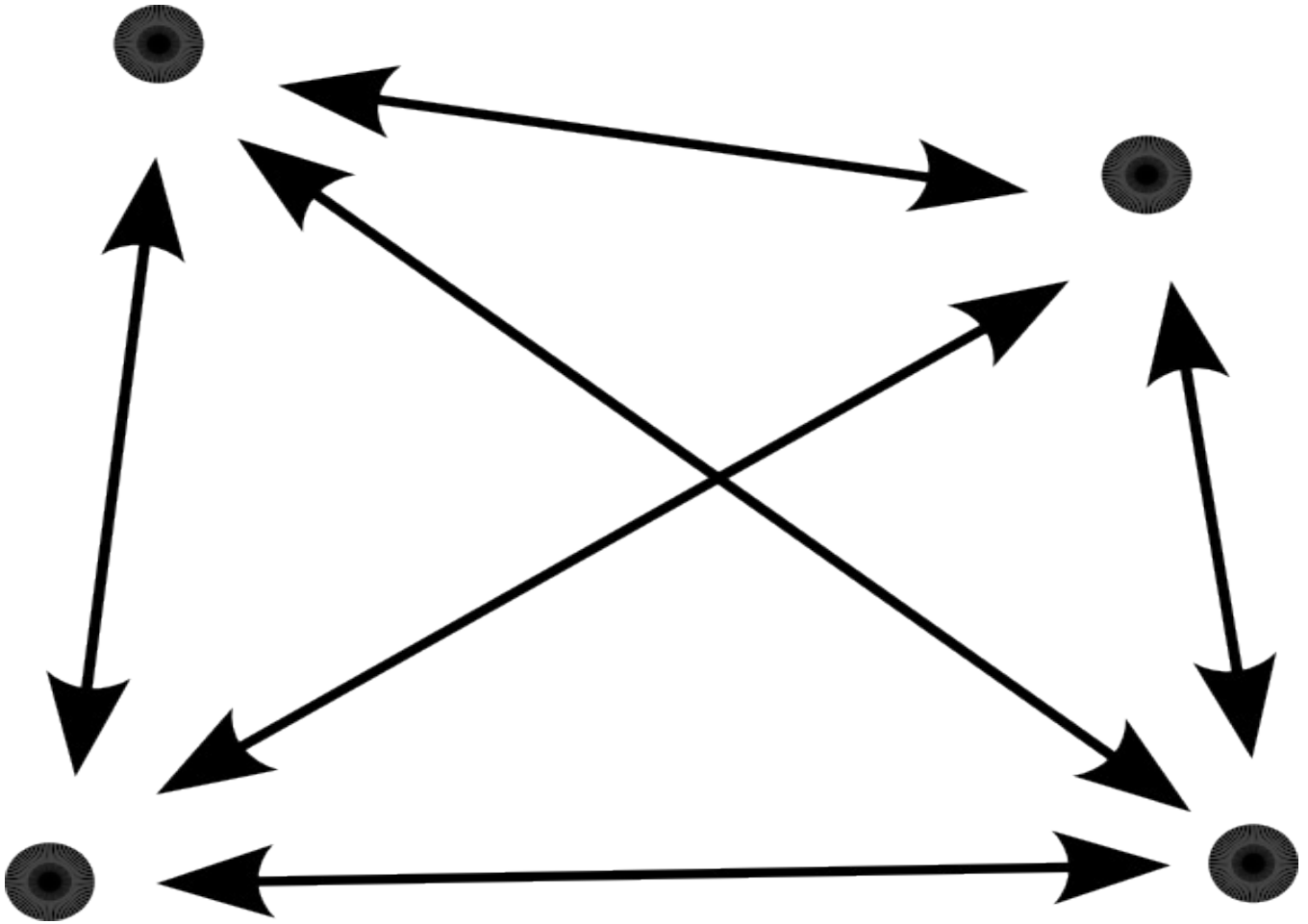
WHY MULTICAST?

chat & social networking =
many-to-many communication

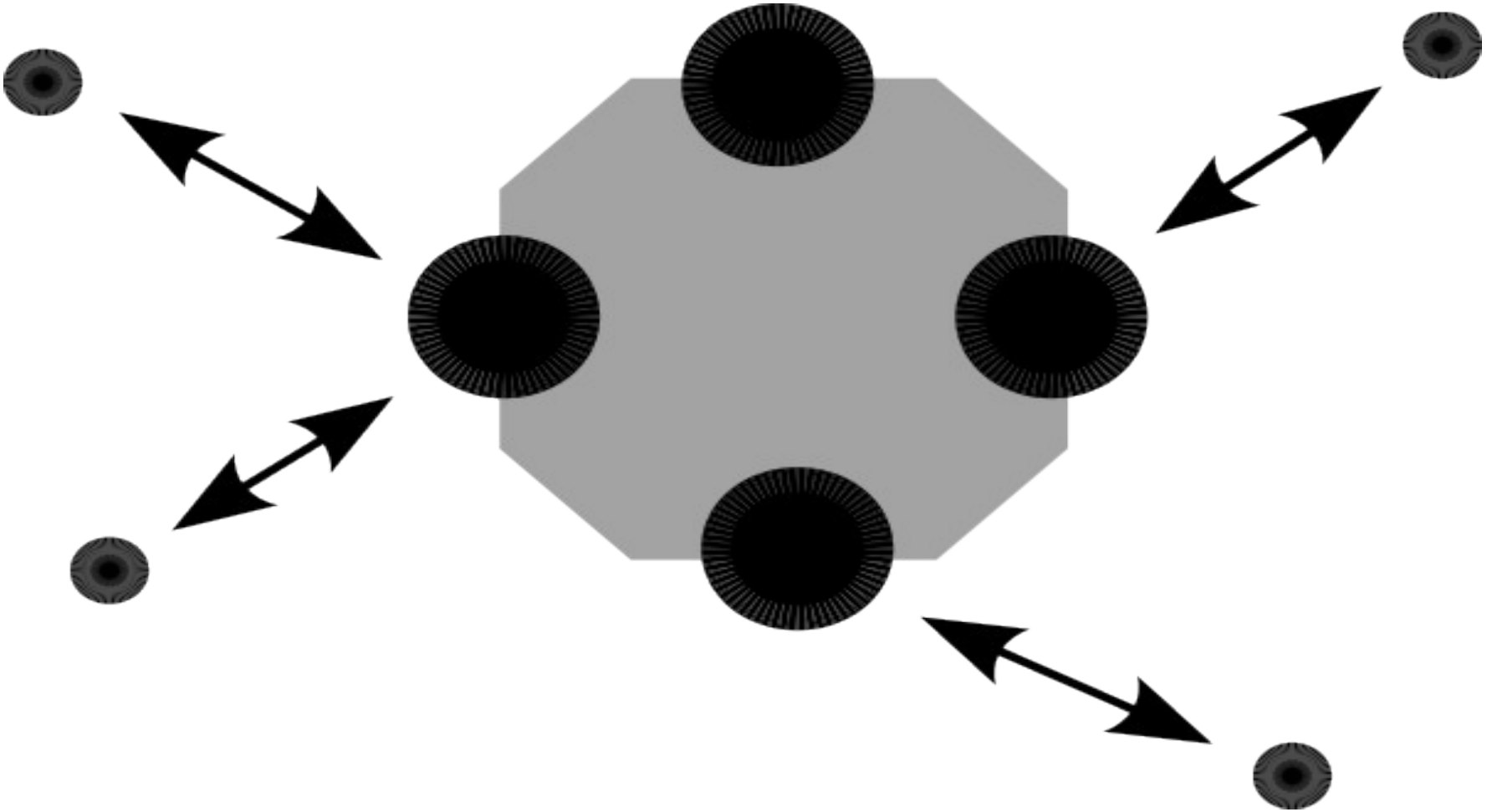
updates, photos, articles...
even profile edits sent to all

everything ready to use on *your* device

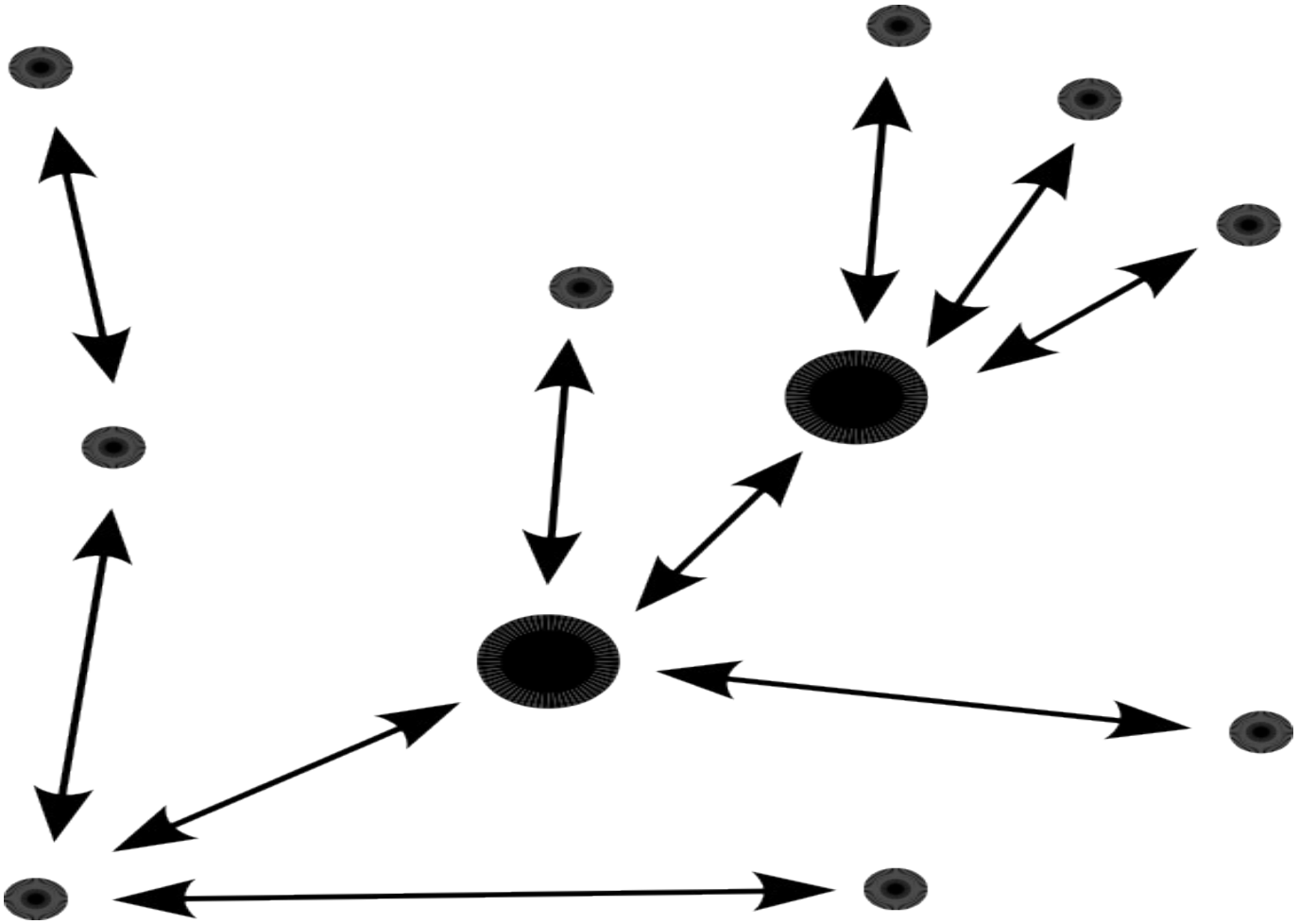
FULL MESH UNICAST, ROUND ROBIN



THE FACEBOOGLE CLOUD



MULTICAST DISTRIBUTION TREE



SCALABILITY & SOCIAL NETWORKING

to make it work.. either
centralize (oh no, PRISM!)
or multicast ...

... like bittorrent
or peer-to-peer TV (streaming)

email #fail
federated social web #fail

SOCIAL GRAPH & ONION ROUTING

combine multicast trees & onion routing

trust relationship between nodes
intermediary nodes agnostic of content

motivation for "servers" as routers:

my server = me
(or a “good friend” of mine in my social graph)

DUMB SERVERS ARE OKAY FOR NOW

speed, reliability, storage space

compensate for offline devices

even if servers are corrupted, they only forward encrypted data – no important role as before

WE'LL MAKE OURSELVES A GNU INTERNET

syncing files between my devices

group communications & data exchanges, social networking

media: photo albums, videos, music

API for GNU social applications

realtime streaming

WE'LL MAKE OURSELVES A GNU INTERNET

but where is the business in it?

is there a business model
for freedom & privacy?

content can be commercial …

… code has to be free

basic civil rights prevail

FREEDOM!

free software

free hardware

certified & sealed

(idea of “certified & sealed computers” is worth a whole presentation by itself)

we need the political vision & will

GIVE US A HAND

secushare.org & gnunet.org are working on

- multicast layer
- distributed data storage
- localhost javascript API

we could use financing, code contribution, interface design, review, promotion ...

IN THE MEANTIME

- use Tor by default
- use Tails, not Ubuntu
- use Privoxy, try Vidalia
- use HTTPS with Certificate Patrol
- try Tor hidden services
- try Retroshare

- fade out PGP and OTR as they show who is talking to whom
- fade out PGP because your private key can give you trouble later (no forward secrecy)

IT'S ABOUT DEMOCRACY

It's not about how much you want to make believe you got nothing to hide. It's about your civic duty to not be a predictable populace.

@lynXintl