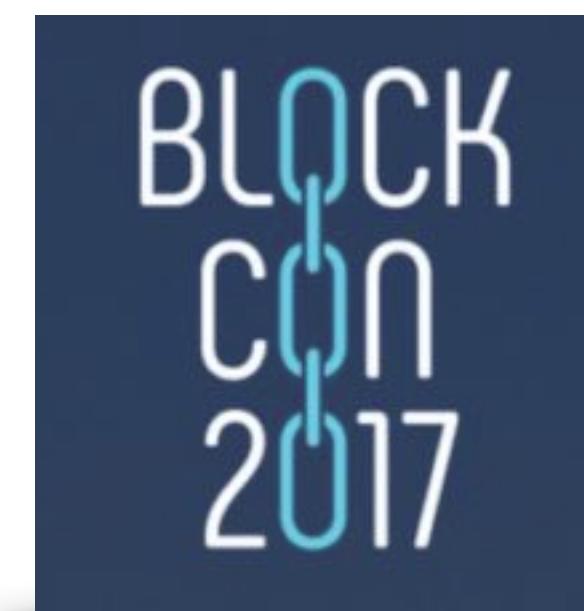


From DNS to DPKI

a.k.a. "Why secure decentralized namespaces are the future"

A presentation by Greg Slepak

at





Greg Slepak

 @taoeffect



Espionage



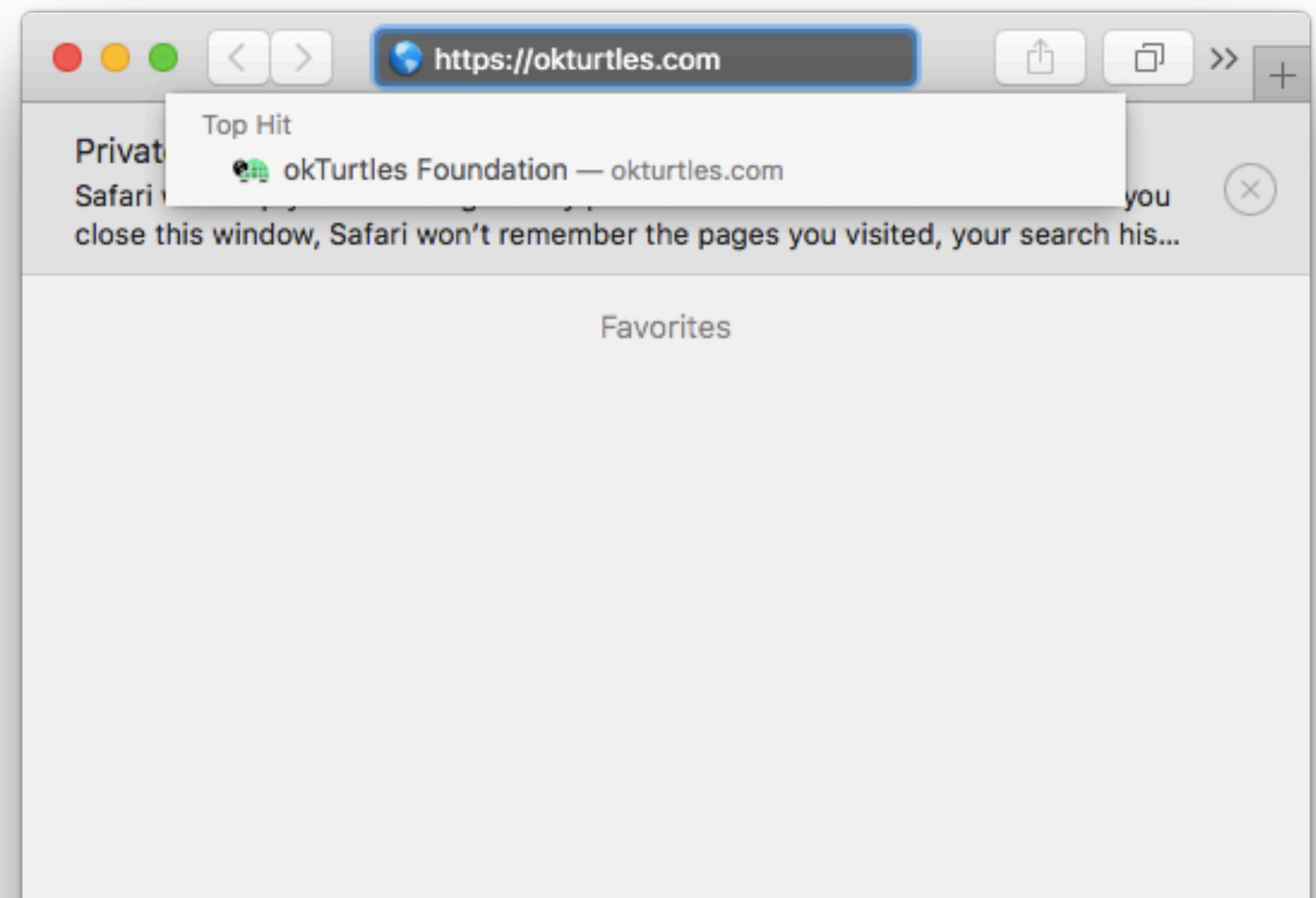
okTurtles

-  DNSChain / DPKI
-  GroupIncome
-  Group Currency

Brief overview of “the problem”

Step 1

user types website domain, hits <Enter>



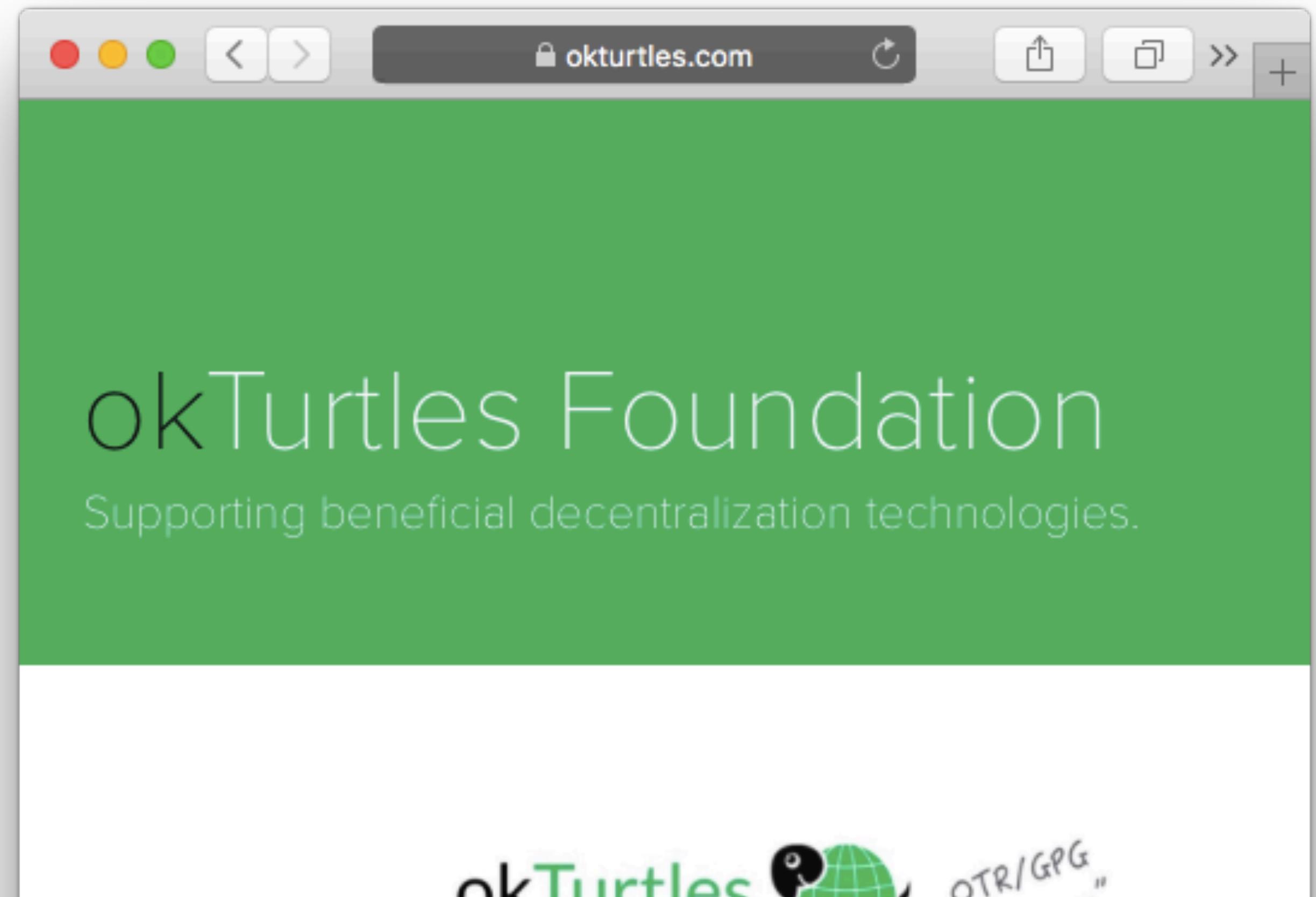
DNS → IP address



IP address → certificate

certificate → SSL/TLS

Step 2



DNS → IP address



IP address → certificate

certificate → SSL/TLS

Step 2

Keychain Access

Click to unlock the System Roots keychain.

Search

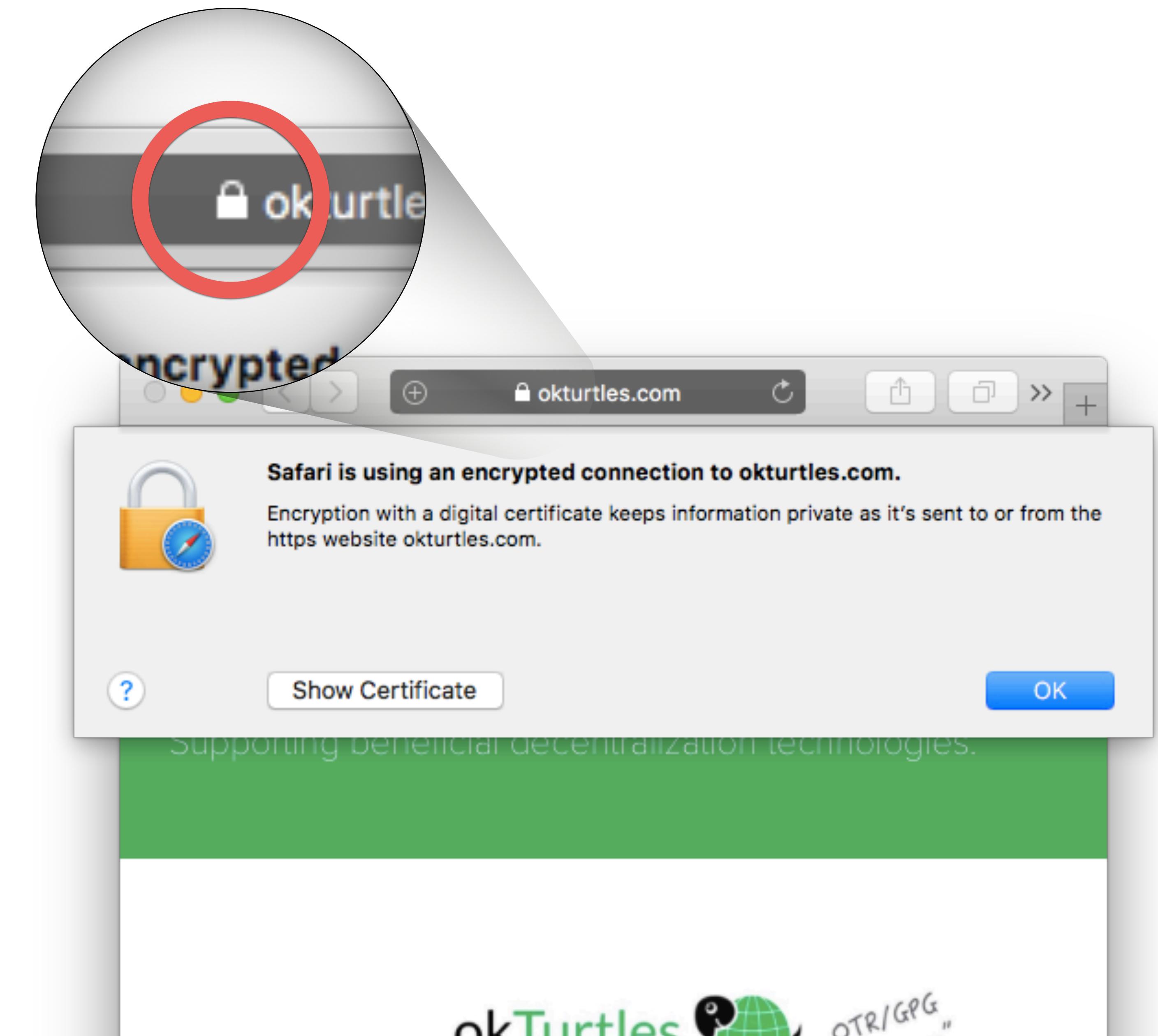
Keychains

- login
- Local Items
- System
- System Roots

AAA Certificate Services
Root certificate authority
Expires: Monday, January 1, 2029 at 12:59:59 AM Central European Standard Time
This certificate is valid

Name	Kind	Date Modified	Expires	Keychain
EE Certification Centre Root CA	certificate	--	Dec 18, 2030, 12:59:59 AM	System Roots
Entrust Root...rtification Authority	certificate	--	Nov 27, 2026, 9:53:42 PM	System Roots
Entrust Root...tion Authority - EC1	certificate	--	Dec 18, 2037, 4:55:36 PM	System Roots
Entrust Root...ation Authority - G2	certificate	--	Dec 7, 2030, 6:55:54 PM	System Roots
Entrust.net C...n Authority (2048)	certificate	--	Dec 24, 2019, 7:20:51 PM	System Roots
Entrust.net C...n Authority (2048)	certificate	--	Jul 24, 2029, 4:15:12 PM	System Roots
ePKI Root Certification Authority	certificate	--	Dec 20, 2034, 3:31:27 AM	System Roots
Federal Common Policy CA	certificate	--	Dec 1, 2030, 5:45:27 PM	System Roots
GeoTrust Global CA	certificate	--	May 21, 2022, 6:00:00 AM	System Roots
GeoTrust Prim...tification Authority	certificate	--	Jul 17, 2036, 1:59:59 AM	System Roots
GeoTrust Prim...ion Authority - G2	certificate	--	Jan 19, 2038, 12:59:59 AM	System Roots
GeoTrust Prim...on Authority - G3	certificate	--	Dec 2, 2037, 12:59:59 AM	System Roots
Global Chambersign Root	certificate	--	Sep 30, 2037, 6:14:18 PM	System Roots
Global Chambersign Root - 2008	certificate	--	Jul 31, 2038, 2:31:40 PM	System Roots
GlobalSign	certificate	--	Mar 18, 2029, 11:00:00 AM	System Roots
GlobalSign	certificate	--	Jan 19, 2038, 4:14:07 AM	System Roots
GlobalSign	certificate	--	Jan 19, 2038, 4:14:07 AM	System Roots
All Items	passwords	--	Dec 15, 2021, 9:00:00 AM	System Roots
>Passwords	passwords	--	Jan 28, 2028, 1:00:00 PM	System Roots
Secure Notes	passwords	--	Jun 29, 2034, 7:06:20 PM	System Roots
My Certificates	certificates	--	Jan 1, 2038, 12:59:59 AM	System Roots
Keys	keys	--	Dec 31, 2037, 4:59:59 PM	System Roots
Certificates	certificates	--	Dec 1, 2031, 2:49:52 PM	System Roots
Hellenic Acad...tions RootCA 2011	certificate	--	May 15, 2023, 6:52:29 AM	System Roots
Hongkong Post Root CA 1	certificate	--	Sep 1, 2019, 2:00:00 AM	System Roots
I.CA - Qualifie...uthority, 09/2009	certificate	--	Jan 16, 2034, 7:12:23 PM	System Roots
IdenTrust Commercial Root CA 1	certificate	--	Jan 16, 2034, 6:53:32 PM	System Roots
IdenTrust Public Sector Root CA 1	certificate	--	Jun 4, 2035, 1:04:38 PM	System Roots
ISRG Root X1	certificate	--	Dec 13, 2037, 9:27:25 AM	System Roots
Izenpe.com	certificate	--	Jan 31, 2018, 12:00:00 AM	System Roots
Izenpe.com	certificate	--	Dec 13, 2037, 9:27:25 AM	System Roots
Izenpe.com	certificate	--	Dec 13, 2037, 9:27:25 AM	System Roots

Step 3



“More than 1200 root and intermediate CAs can currently sign certificates for any domain and be trusted by popular browsers.”

<http://www.ietf.org/mail-archive/web/therightkey/current/msg00745.html>

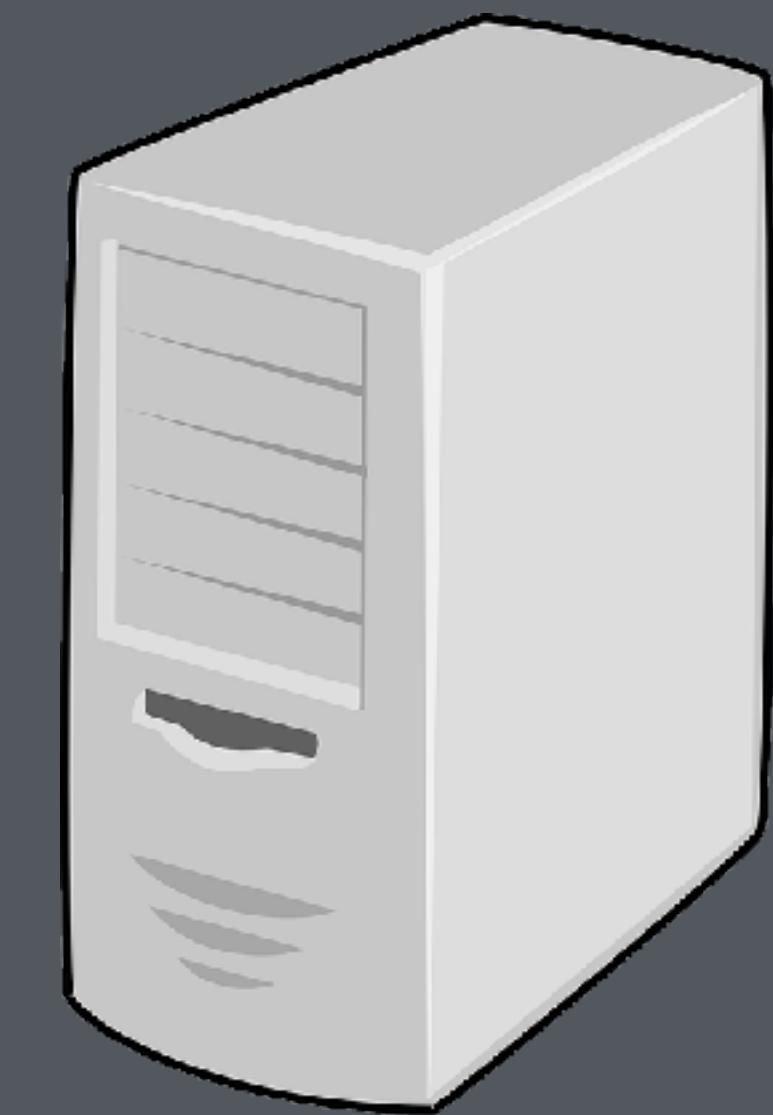


fnsabook

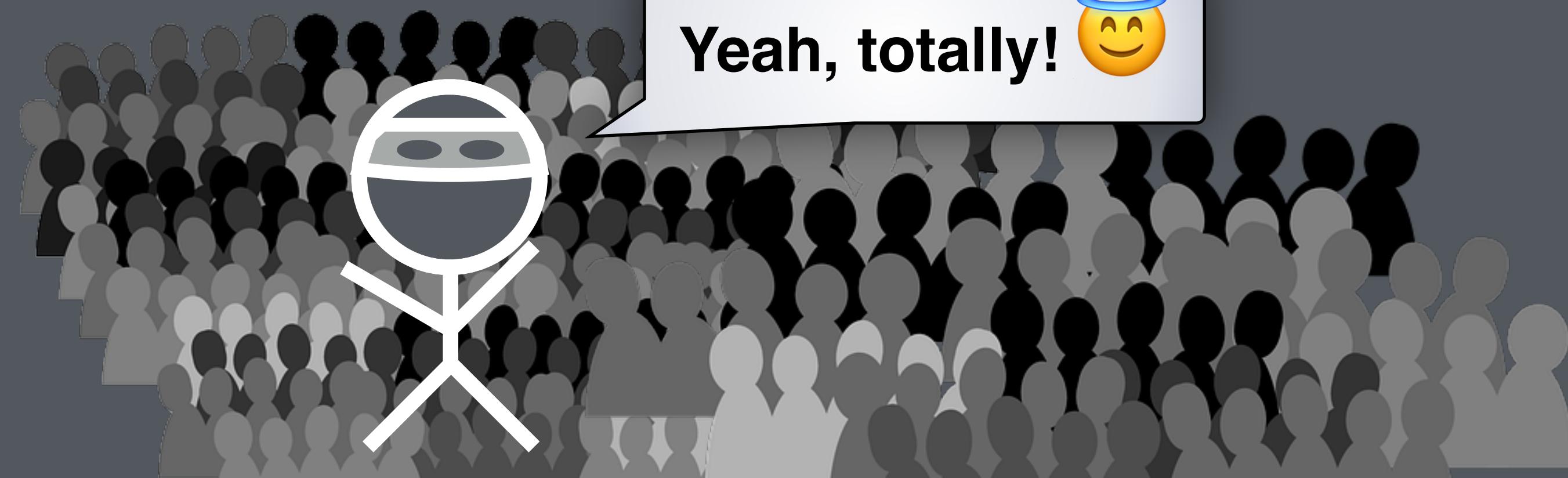
Man-In-The-Middle

HTTPS/TLS/SSL
(SIMPLIFIED)

Is this legit?



Yeah, totally! 😊



TLS/SSL
VERIFIED

You are connected to
facebook.com
which is run by
(unknown)

Verified by: DigiCert Inc



The connection to this website is secure.

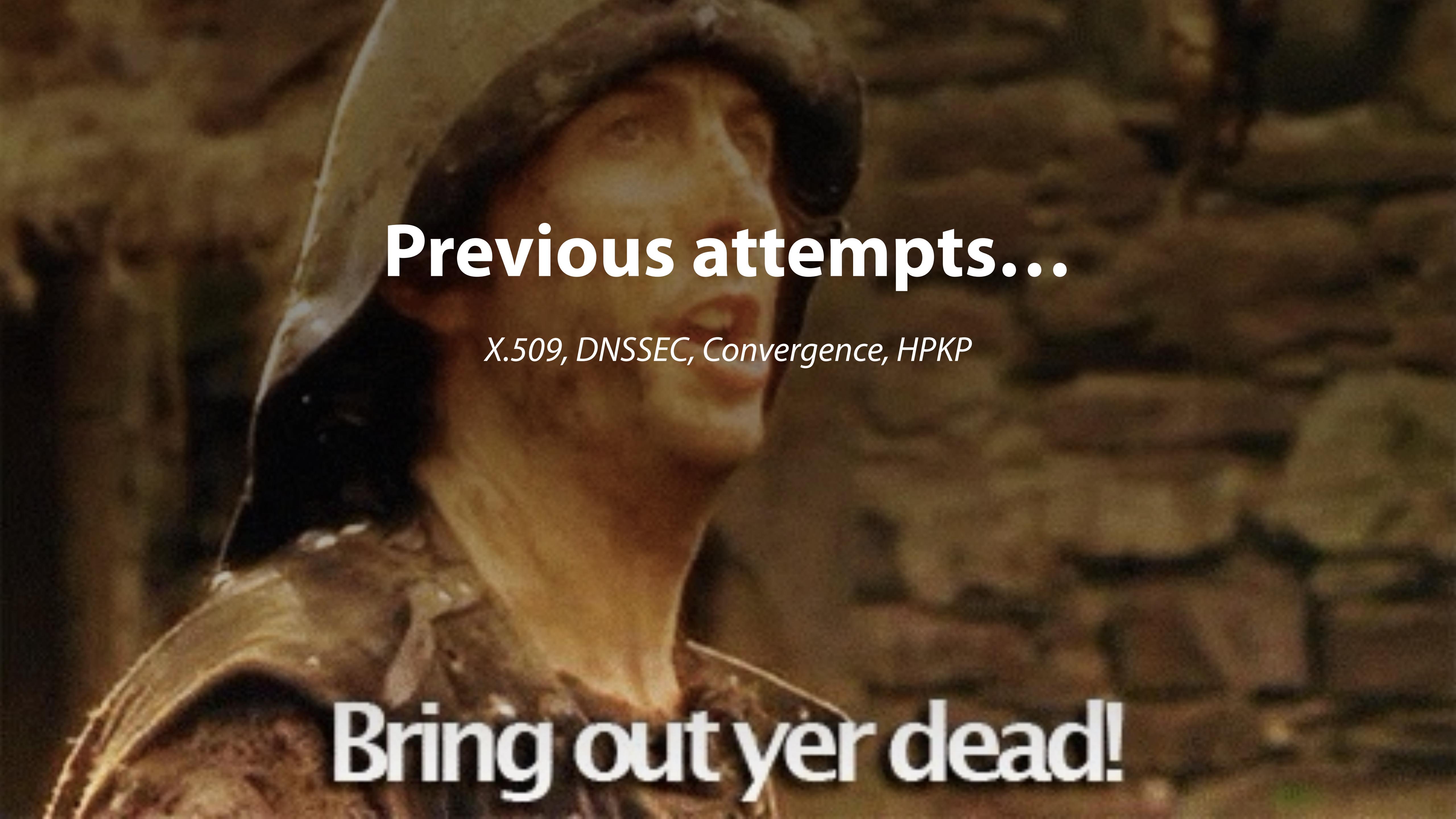


More Information...

Let's clearly define **The Problem™**

The Problem™

1. **Who can define *your identity* to strangers when you're not there?**
2. Is there *a good reason* to *trust* those in (1)?
3. Is the mechanism *usable*?



Previous attempts...

X.509, DNSSEC, Convergence, HPKP

Bring out yer dead!

X.509

(we just covered it)

DNSSEC

DNSSEC

is complicated

IETF standards [edit]

- [RFC 2535](#) Domain Name System Security Extensions
- [RFC 3833](#) A Threat Analysis of the Domain Name System
- [RFC 4033](#) DNS Security Introduction and Requirements (*DNSSEC-bis*)
- [RFC 4034](#) Resource Records for the DNS Security Extensions (*DNSSEC-bis*)
- [RFC 4035](#) Protocol Modifications for the DNS Security Extensions (*DNSSEC-bis*)
- [RFC 4398](#) Storing Certificates in the Domain Name System (DNS)
- [RFC 4470](#) Minimally Covering NSEC Records and DNSSEC On-line Signing
- [RFC 4509](#) Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- [RFC 5155](#) DNSSEC Hashed Authenticated Denial of Existence
- [RFC 6781](#) DNSSEC Operational Practices, Version 2

DNSSEC is Expensive To Deploy

DNSSEC is harder to deploy than TLS. TLS is hard to deploy (look how many guides sysadmins and devops teams write to relate their experience doing it). It's not hard to find out what a competent devops person makes. Do the math.

— Thomas & Erin Ptacek

DNSSEC

is unnecessary

DNSSEC is Unnecessary

All secure crypto on the Internet assumes that the DNS lookup from names to IP addresses are insecure. Securing those DNS lookups therefore enables no meaningful security. DNSSEC does make some attacks against insecure sites harder. But it doesn't make those attacks *infeasible*, so sites still need to adopt secure transports like TLS. With TLS properly configured, DNSSEC adds nothing.

— Thomas & Erin Ptacek

**“It’s essentially removing the authenticity element from SSL
and using the one from DNSSEC instead.”**

— Moxie

DNSSEC

is broken

next slide might take a second to load...

Major DNSSEC Outages and Validation Failures

Updated: May 14, 2017

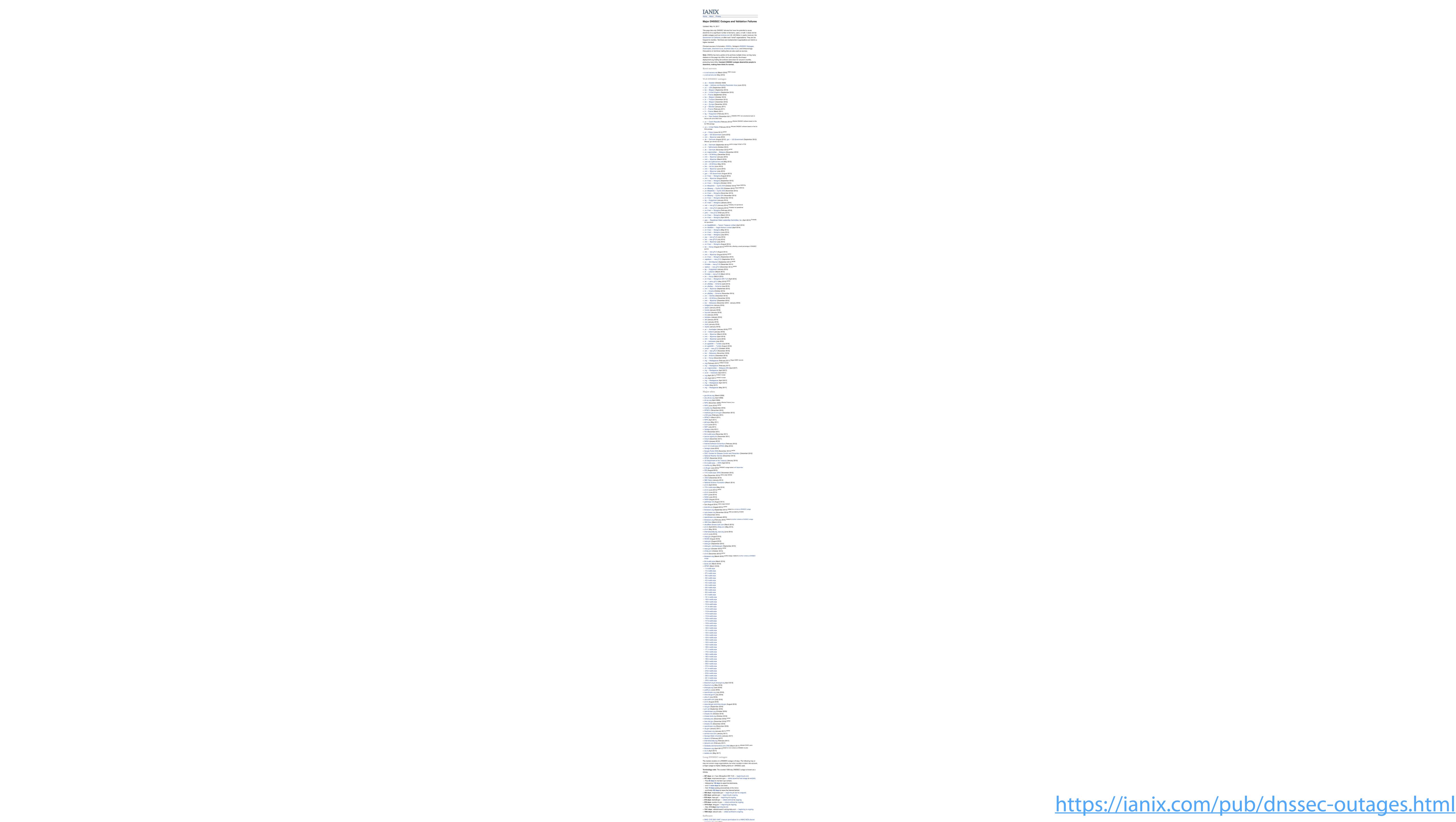
This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as [dominos.com](#) (\$1.425 Billion in yearly revenue), the [Government of California](#), or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: [DNSViz](#), Verisign's [DNSSEC Debugger](#), [Zonemaster](#), [dnscheck.iis.se](#), [dnscheck.labs.nic.cz](#), and Unbound logs. Discussions on technical mailing lists are also used as sources.

Note: DNSViz has lost a portion of its archives multiple times, turning many citations on this page into 404s. And until recently, the dnssec-deployment.org mailing list archives were down for around 5 months, producing more 404s. **Constant DNSSEC outages desensitize people to downtime, making them think it's normal.**

Root servers

- [m.root-servers.net](#) (March 2010) PMTU issues



DNSSEC

is less secure than X.509

slower. But if the basic structure is the same, the next obvious question is whether there might be any improvement in how the DNSSEC trust relationships work compared to the current CA system.

It turns out that in the case of DNSSEC, there are three classes of people that we have to simultaneously trust:

(Registrars, TLDs, and ICANN)

— Moxie

DNSSEC is the world's most ambitious key escrow scheme: **a backdoor that hands over control of Internet cryptography to world governments**. Thankfully, it's also a total market failure. We should hope it stays that way.

— Thomas & Erin Ptacek

Convergence / Perspectives

is a real improvement, however...

	NSC	IR	GA	TA	NTTP	IS	US
Certificate Transparency	Yes	Yes	Yes	Yes	Yes	Yes	Yes(4)
DANE (but see note (7))	No	Yes	Yes	Yes	No	Yes	No (5)
CAA (1)	No	Yes	No	No	No	Yes	No (5)
Pinning	Yes	No	Yes (2)	Yes (2)	Yes	Yes (3)	No (6)
Convergence	No	No	No	Yes	No	No	Yes
TACK	Yes	No	Yes (2)	Yes (2)	No	Yes (3)	No (6)

NSC (No side-channels): our experiments show that side-channel requests to third parties during the SSL handshake (e.g. OCSP checks) fail at least 1% of the time, often a great deal more, depending on what protocol they use. This level of failure makes it impossible to hard fail with protocols that use side channels.

IR (Instant recovery from loss of key): if the server loses its private key, can it immediately roll out a new certificate?

GA (Detects Global Attack): if the server is replaced by an evil server that everyone sees, does the protocol protect clients?

TA (Detects targeted attack): if the server is replaced by an evil server (or MitM) for one person or a small number of people, can the protocol protect those people?

NTTP (No trusted third parties): does the protocol avoid the need for the client to trust a third party?

IS (Instant startup): can a new server use a new certificate immediately and be trusted by clients?

US (Unmodified Servers): can it be used without server changes?

“Rather than employing a traditionally hard-coded list of immutable CAs, Convergence allows you to configure a dynamic set of Notaries which use network perspective to validate your communication.”

Misleading.

99.9% of users won't know what notaries are or how to select them.

In practice, there will be a hard-coded list of CAs.

The improvement comes from the existence of **consensus**.

Consensus:

When a **group** of independent entities **agree**¹ on a decision
(e.g. if a key is valid) **by some voting threshold**²

¹The voting mechanism can be very different, but this idea is the same

²Typically greater than 50%. See:

<https://groupincome.org/2016/06/what-makes-a-good-voting-system/>

<https://groupincome.org/2016/09/deprecating-mays-theorem/>

99.9% of users won't know what notaries are or how to select them.

In practice, there will be a hard-coded list of CAs.

The improvement comes from the existence of **consensus**.

Convergence / Perspectives

is ineffective against server-side MITM

(nothing securing connection from notaries to server)

Pinning (HPKP/TACK)

is difficult to use

Pinning (HPKP/TACK)

is ineffective against MITM on first visit

Pinning (HPKP/TACK)

is broken for users with broken clocks

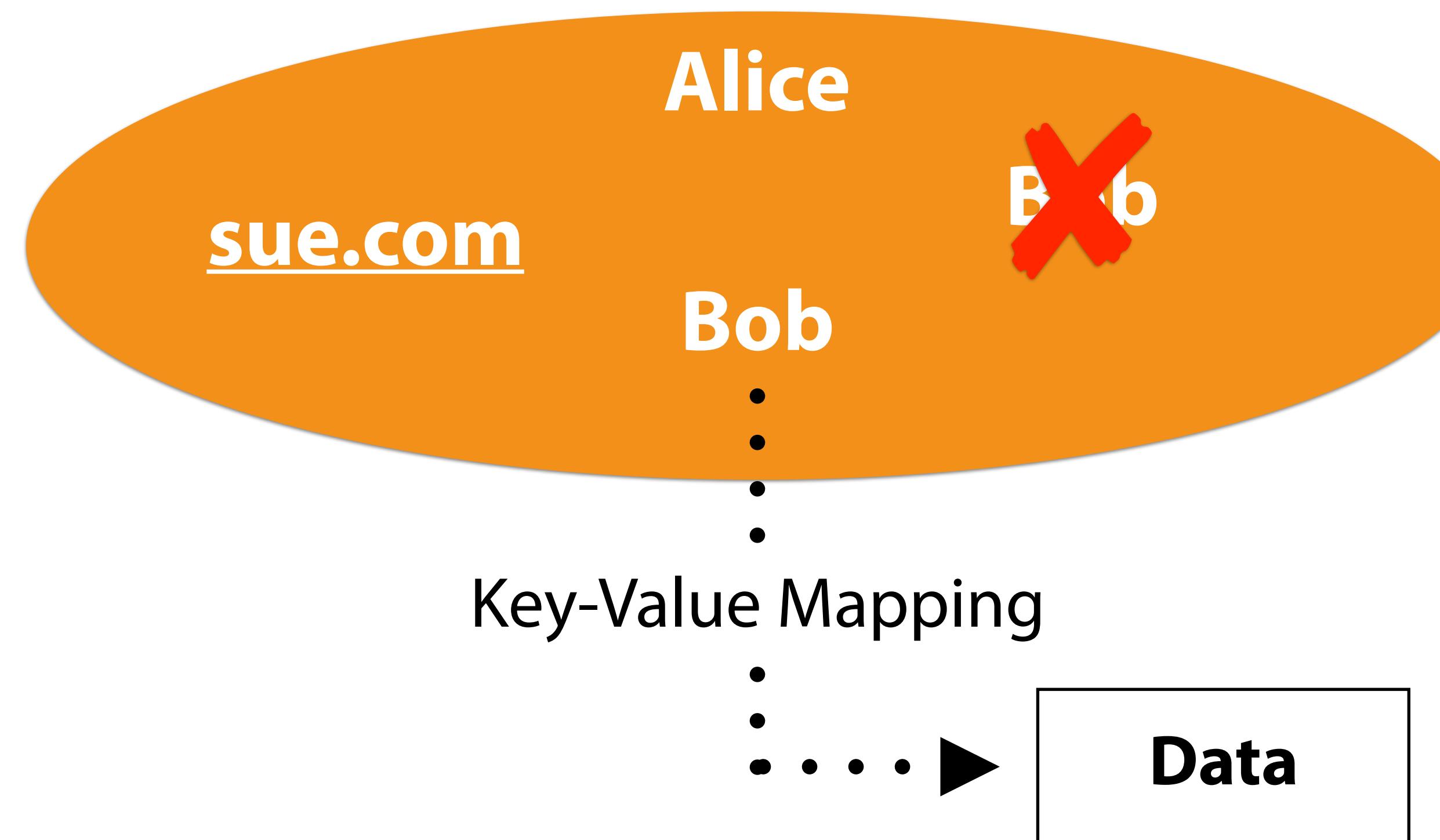
What are their answers
to The Problem™?

Answers to **The Problem™**

	Who can define your identity?	Reason to trust?	Usable?
X.509	Governments, CAs	None	Yes
DNSSEC	Governments, registrars, TLDs, ICANN	None	No
Convergence	nation-state, colluding notaries	Potential to choose consensus group	Yes
HPKP	the CA you picked (if you picked one) (and hackers)	TOFU-based, CA chosen by you	No

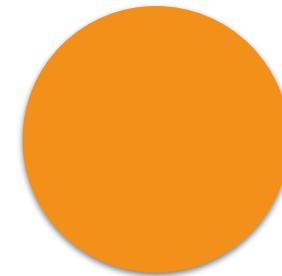
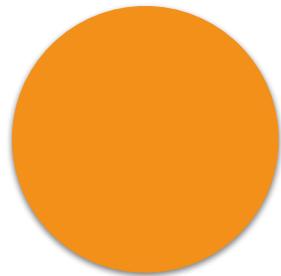
Namespaces

What is a namespace?



Today

DNS — — — — X.509



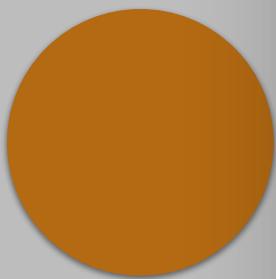
(This is why DNSSEC
is unnecessary)

Notice: neither DNS nor X.509 enforce
unique key-value mapping.

- **dig apple.com** can return arbitrary results
- CAs can issue arbitrary certificates for the same domain

There is no consensus on what the mapping should be!

DNS –



Who should decide what the mapping should be?

Psst... You!

(The person who registered it!)

(THIS IS WHY DNSSEC
is unnecessary)

**There is no consensus on what the
mapping should be!**

**Centralized
Namespaces**

vs

**Decentralized
Namespaces**

Centralized Namespaces

vs

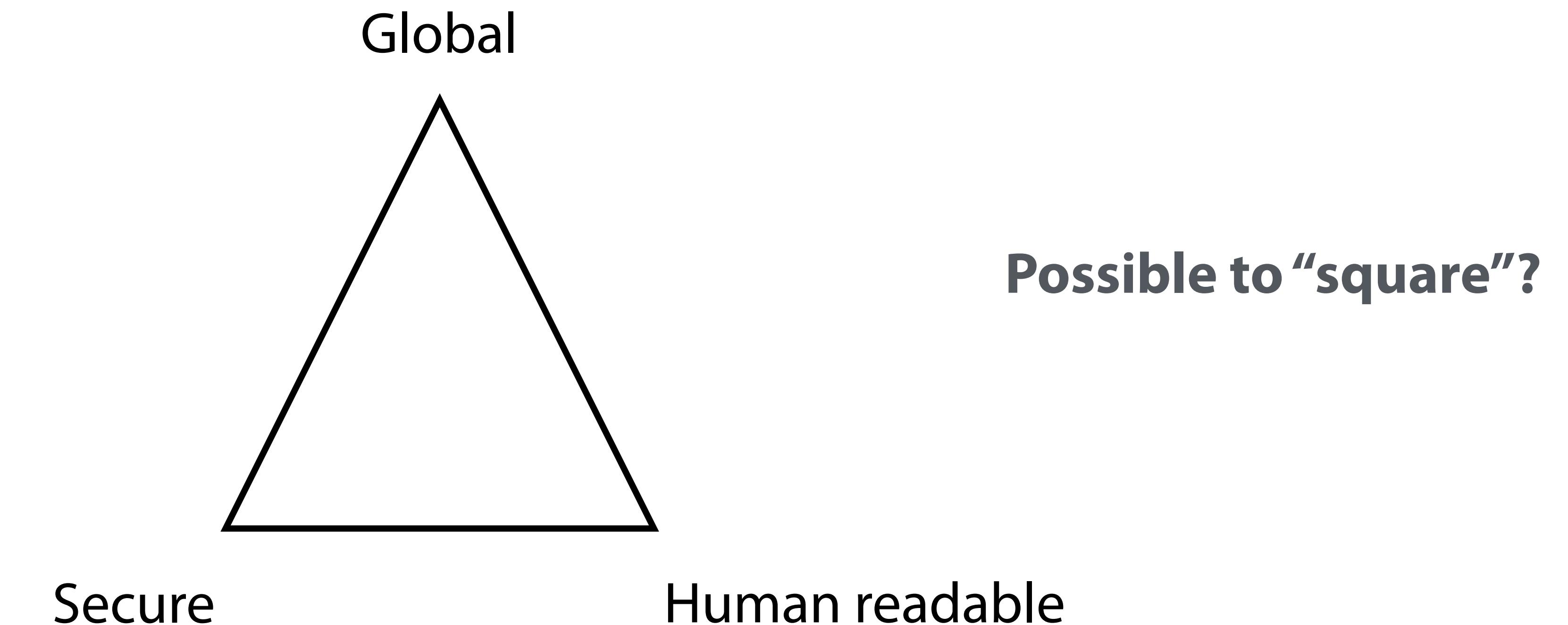
Decentralized Namespaces

- Who controls mappings? **Not you.**
- **Incapable** of providing ownership of an identifier
- **Incapable** of censorship-resistance

- Real ownership and censorship-resistance
- Who controls mappings? **You.***
- The Internet requires it

* As long as they remain decentralized.
See **consensus capture**.

Zooko's Triangle



New attempts! 😊🙌

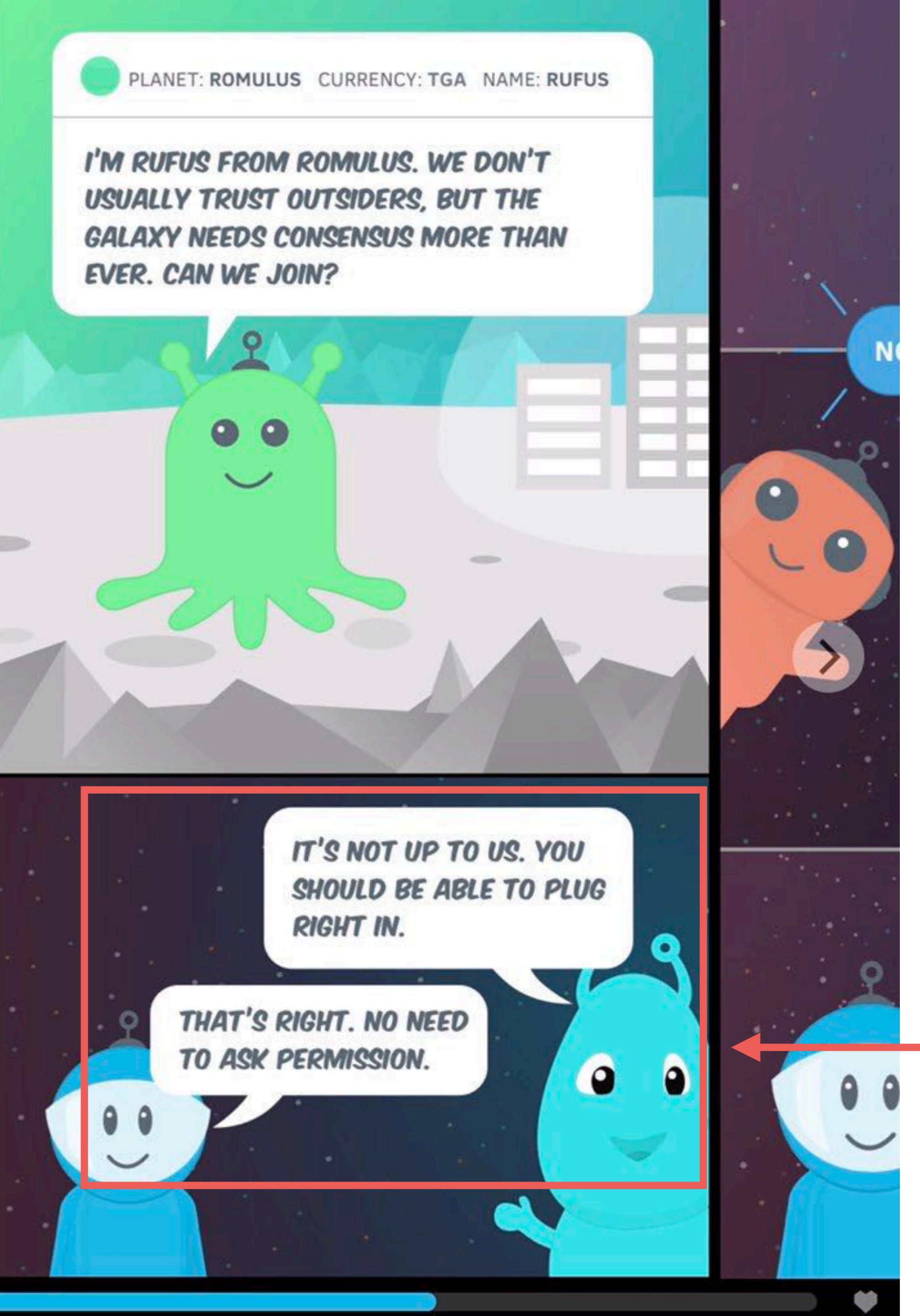
Certificate Transparency, Key Transparency, CONIKS, DPKI and SCP

Long story short...

	Google's CT	Google's KT	CONIKS	DPKI
MITM-detection				
MITM-prevention			(*)	
Internet scalable				
Economically backed security				
Censorship resistant				
DoS resistant				

(*) MITM-prevention in CONIKS depends on novel zero-knowledge proof cryptography that few have verified. Assuming it Works As Advertised, and assuming gossip is successful, and assuming a single entity does not control the server and all messenger implementations using it, it should be capable of preventing MITM attacks.

Stellar Consensus Protocol (SCP)



Greg Slepak
@taoeffect

@JedMcCaleb @iang_fc @bascule Stellar's marketing is grossly misleading on this point. "No need to ask permission [to *listen*!]"

Danger!

Don't break the Internet!

< Date > < Thread >

[Ilc] Genuine concern: is the purpose of this group to create an Internet-cartel?

Tao Effect <contact@taoeffect.com> | Thu, 16 February 2017 06:30 UTC | [Show header](#)

Hi list,

Judging by the name of this group I will not be surprised if this email is simply ignored, but I'm obligated by conscience to voice my concern, if only so that future historians can search these archives and see that yes, someone did contact this group and ask them if they were aware of the consequences, i.e. the high likelihood of turning the Internet back into 20th century cable news.

It is not clear to me, from the name of this working group, whether it understands the meaning of "consensus".

My OS X dictionary says:

> < Thread >

cern: is the the purpose of this group to create an Internet-cartel?
aoeffect.com> | Thu, 16 February 2017 06:30 UTC | Show header

ne of this group I will not be surprised if this email is simply ignored
conscience to voice my concern, if only so that future historians can
see that yes, someone did contact this group and ask them if they were
es, i.e. the high likelihood of turning the Internet back into 20th c.

This is why DPKI explicitly allows
arbitrary consensus protocols.*

*As long as they fit the **mathematical** notion of decentralization.

Decentralized Public Key Infrastructure (DPKI)

DPKI

is different
has to be different

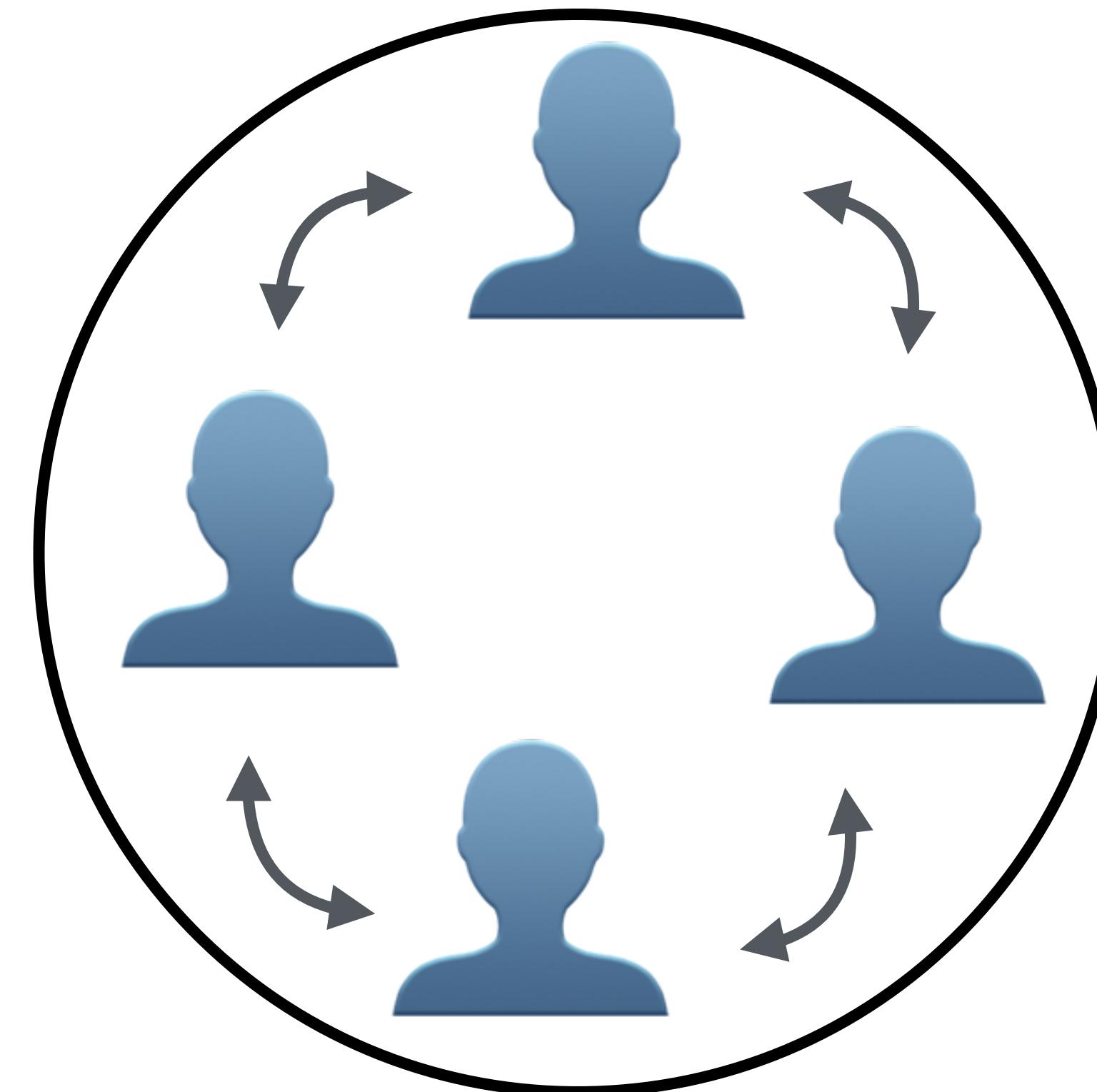
DPKI

because it recognizes consensus capture

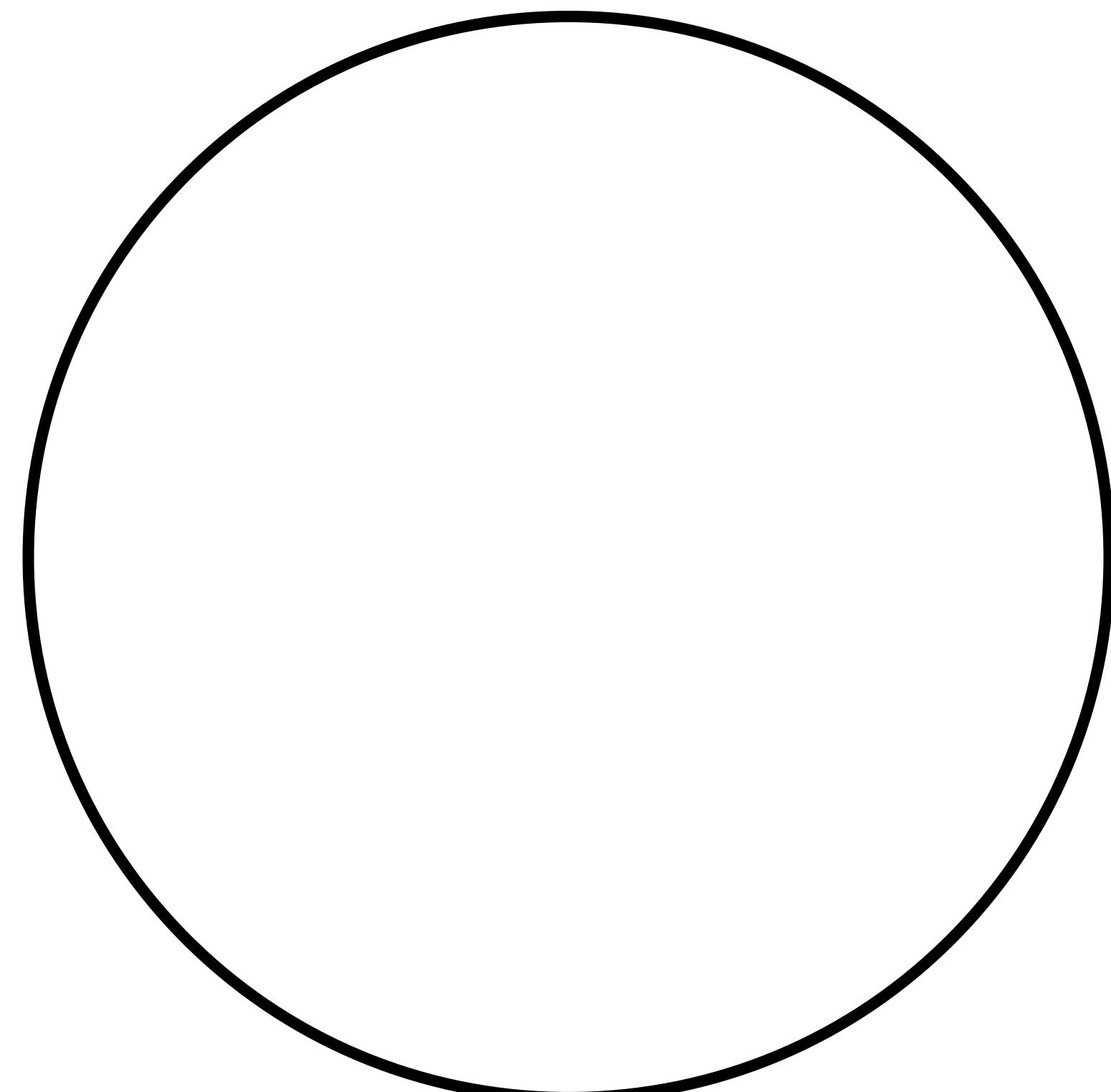
Consensus Capture

Consensus Capture

Our consensus group:

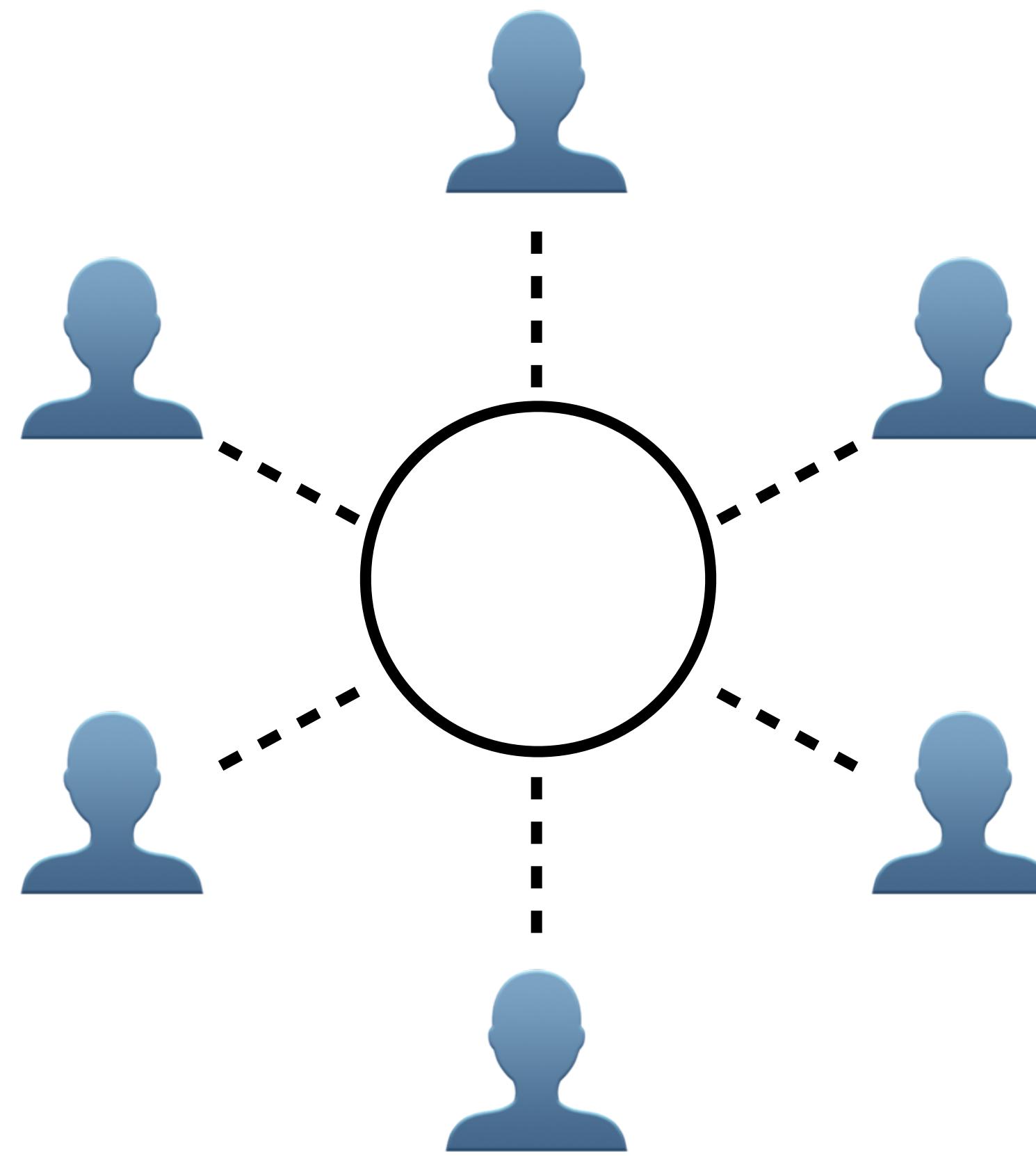


Consensus Capture



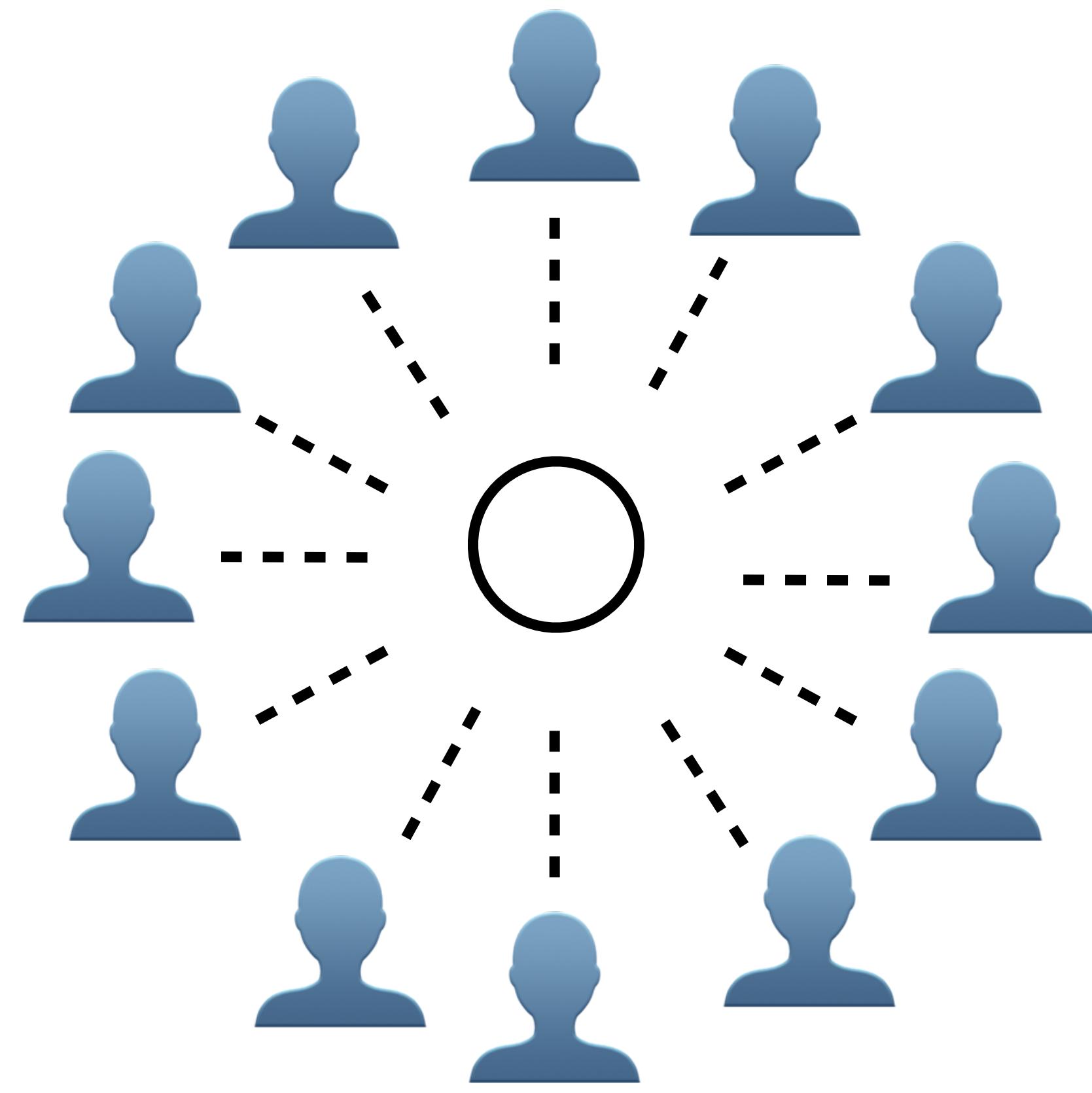
Consensus participants:
100%

Consensus Capture

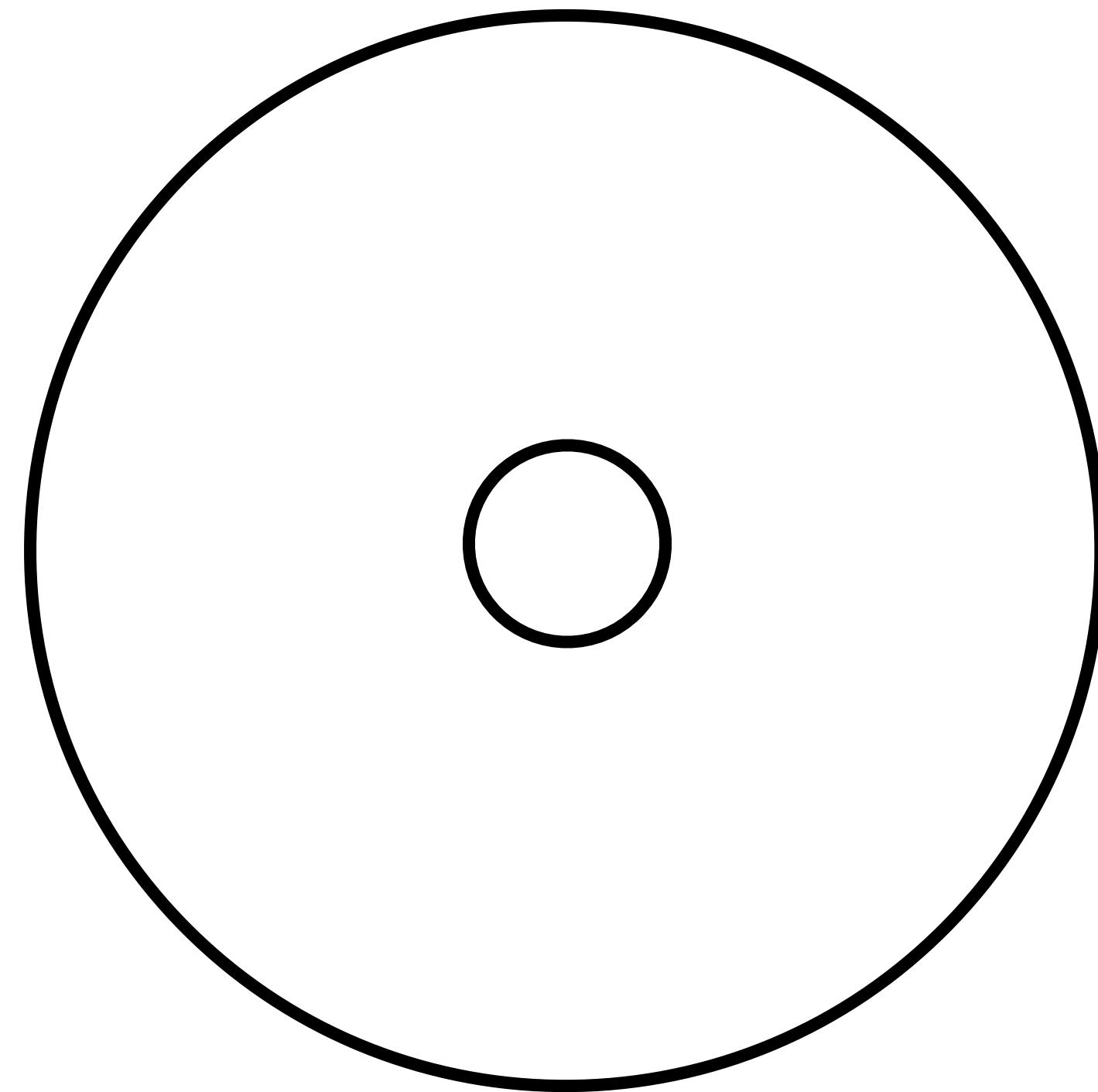


Consensus participants:
40%

Consensus Capture

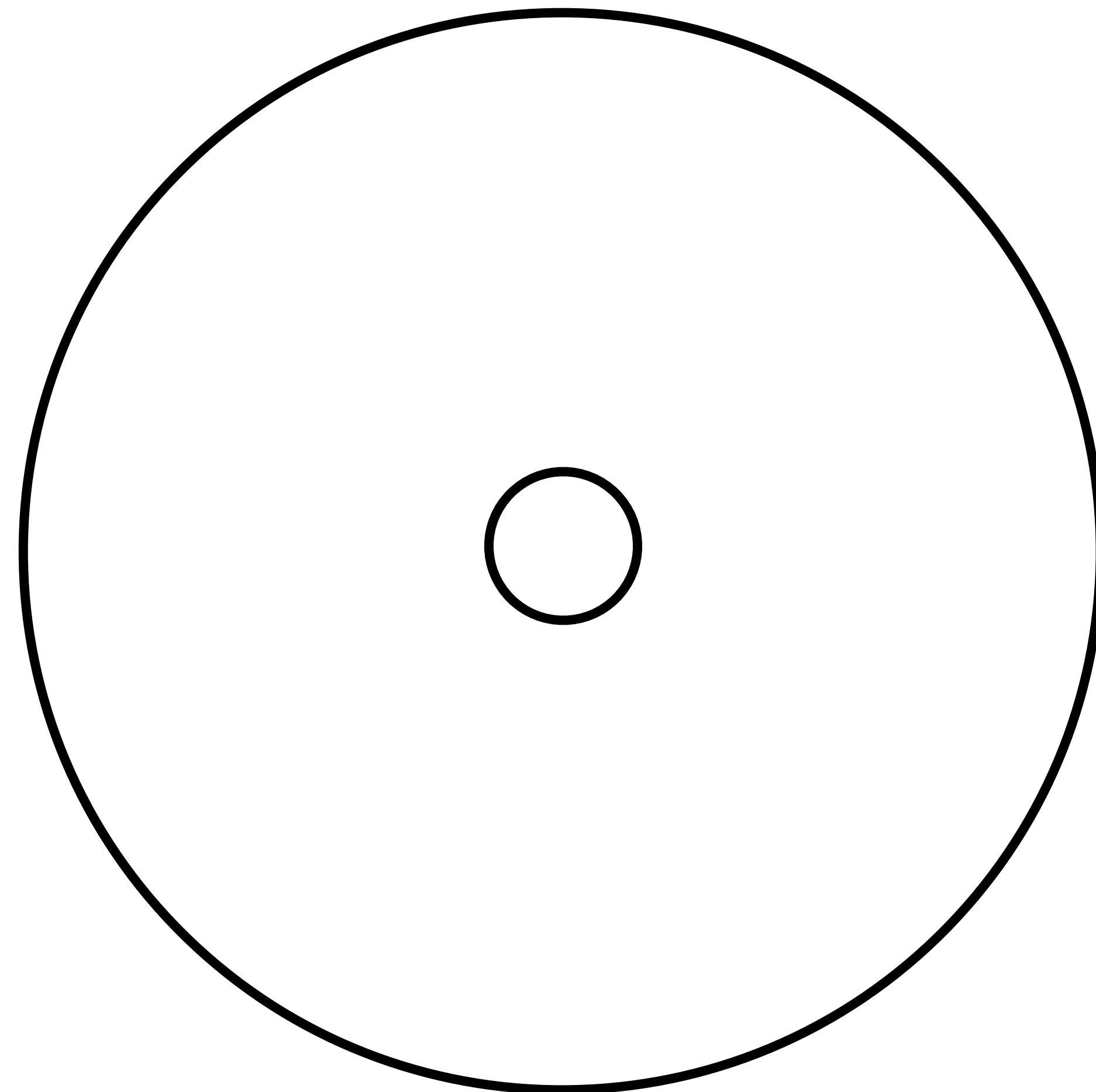


Consensus Capture



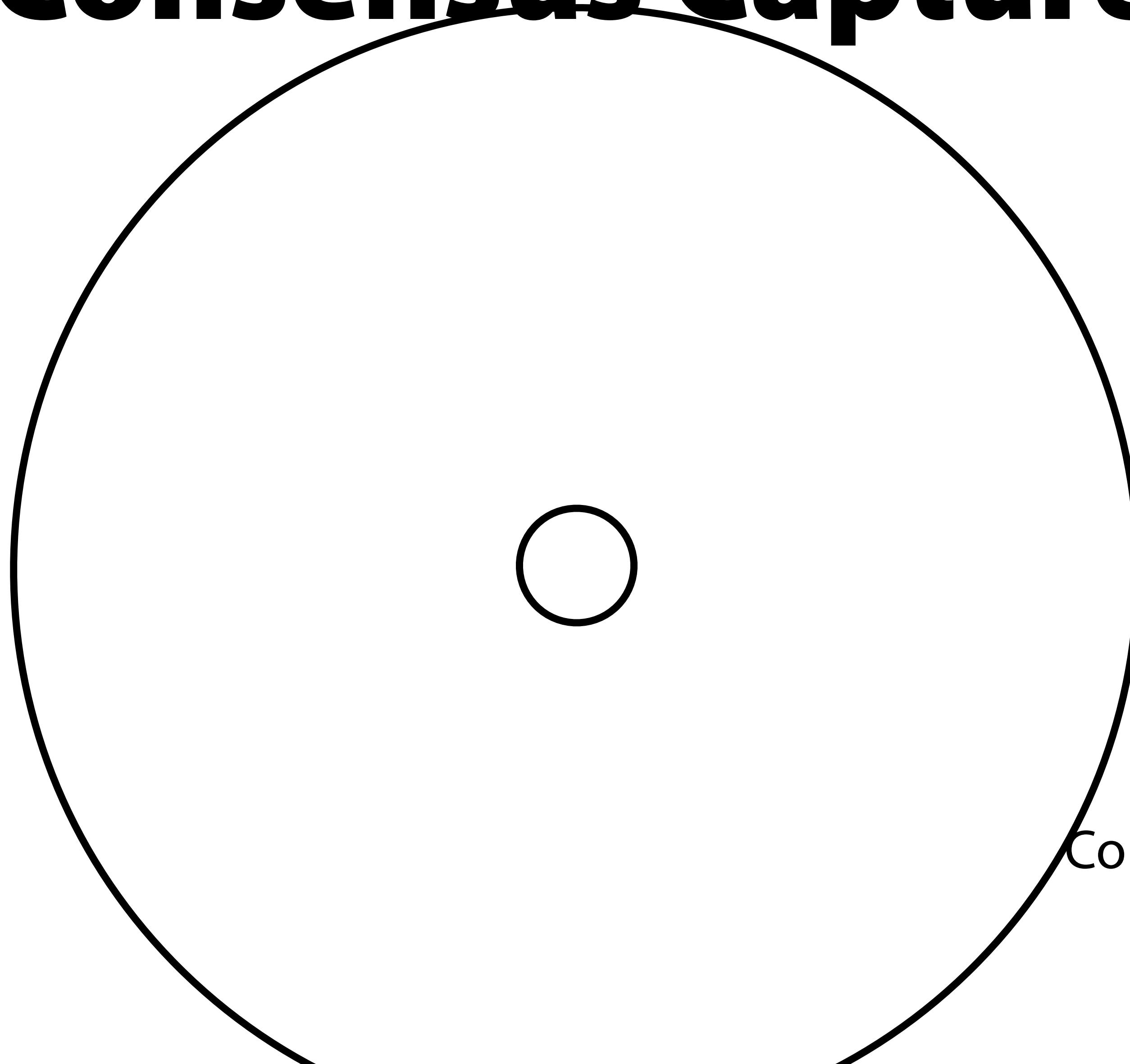
Consensus participants:
25%

Consensus Capture



Consensus participants:
5%

Consensus Capture



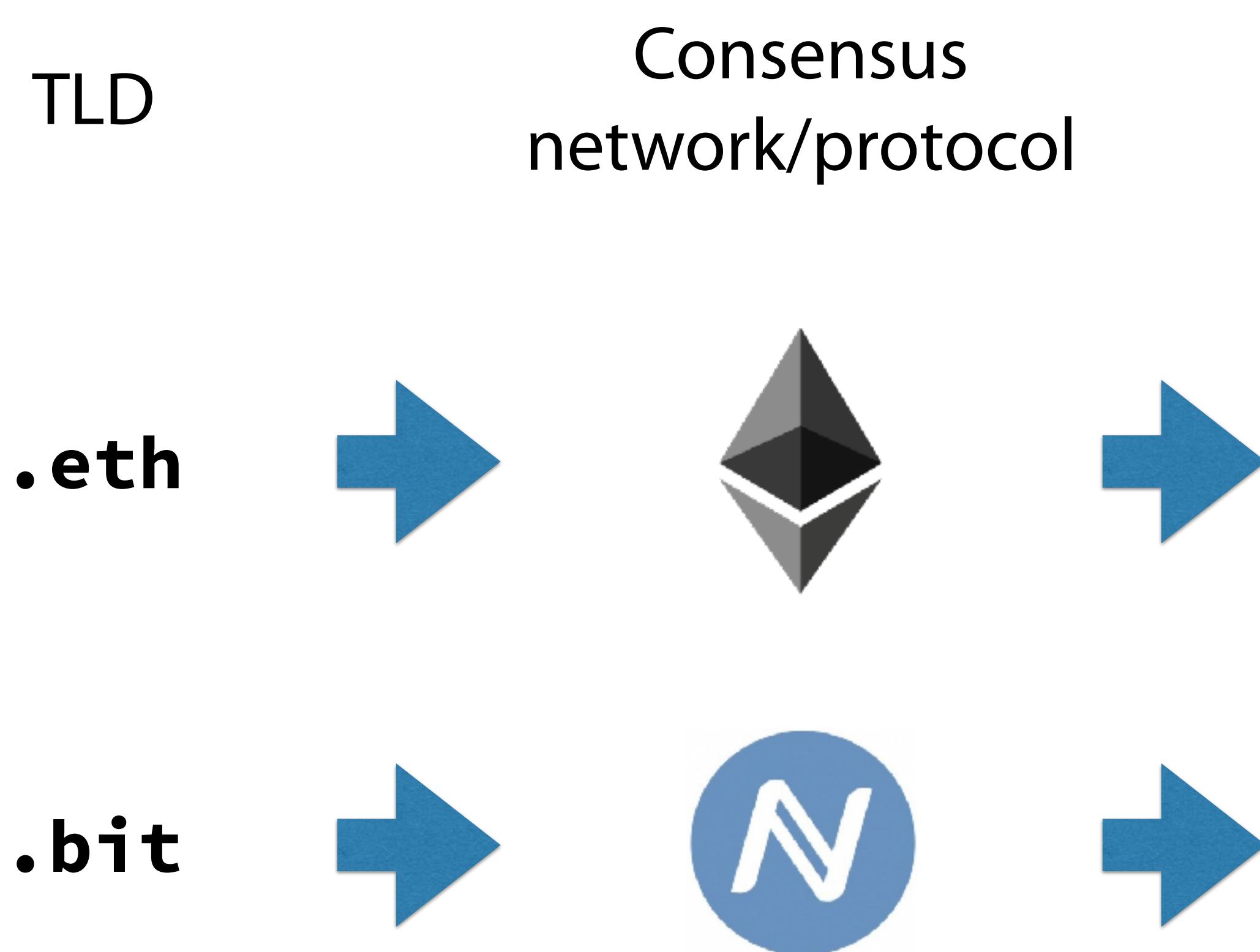
Consensus participants:
1%

DPKI

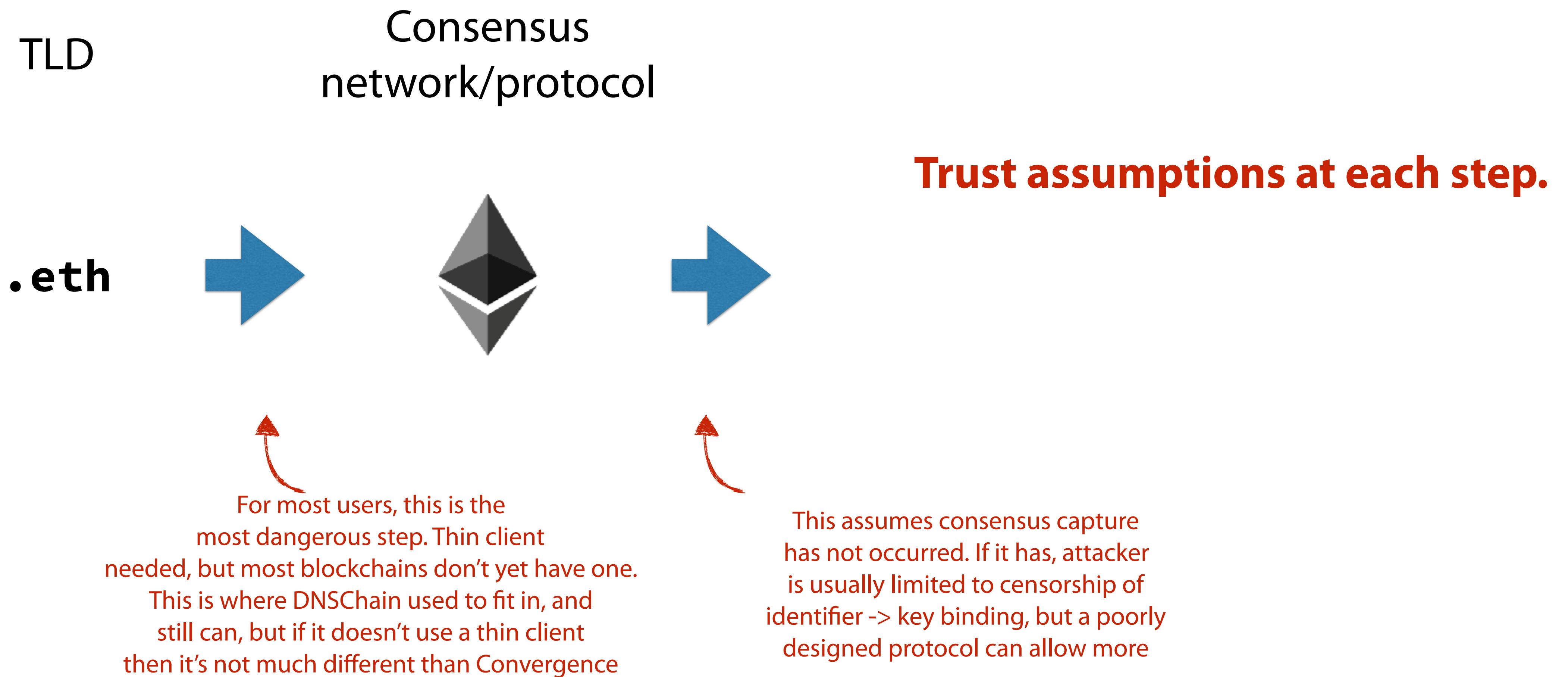
does not specify consensus
is a protocol *for* consensus protocols

DPKI in 2 Parts

Part 1: DPKI namespaces



Part 1: DPKI namespaces

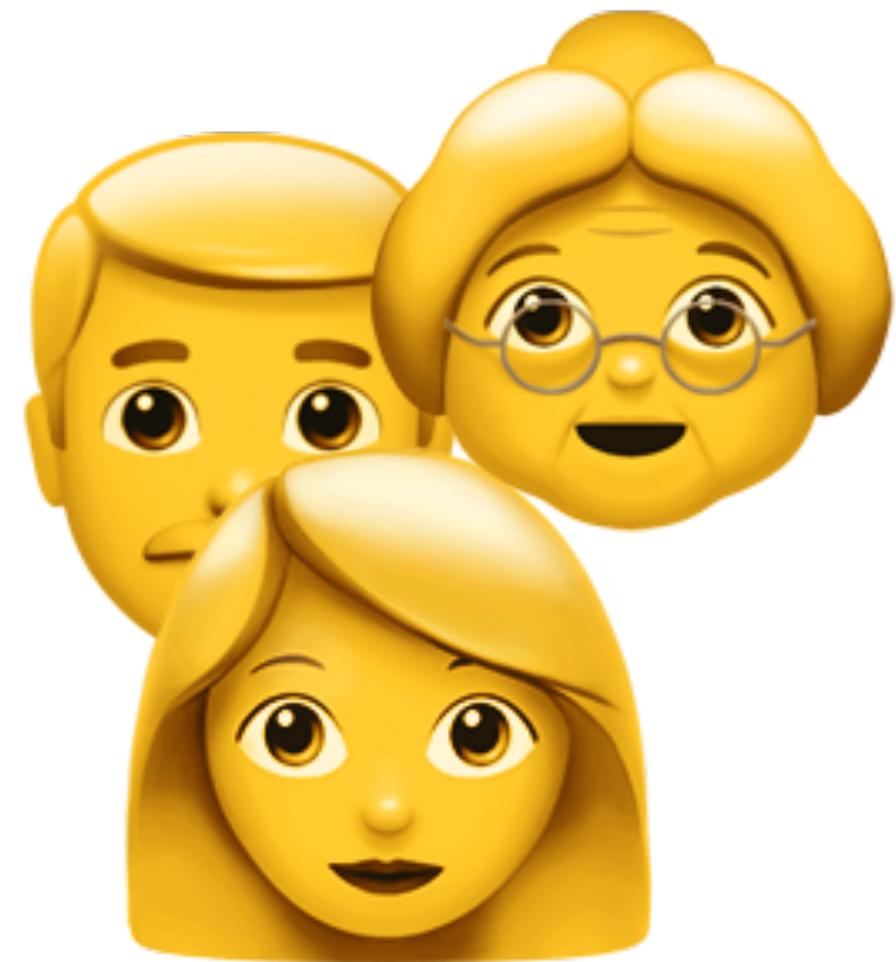
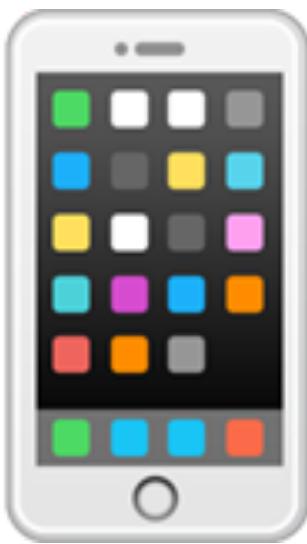


Part 2: Identifier lifecycle

Loss/recovery



Additional devices



More info:
Rebooting Web-of-Trust + DID Spec.

Answers to **The Problem™**

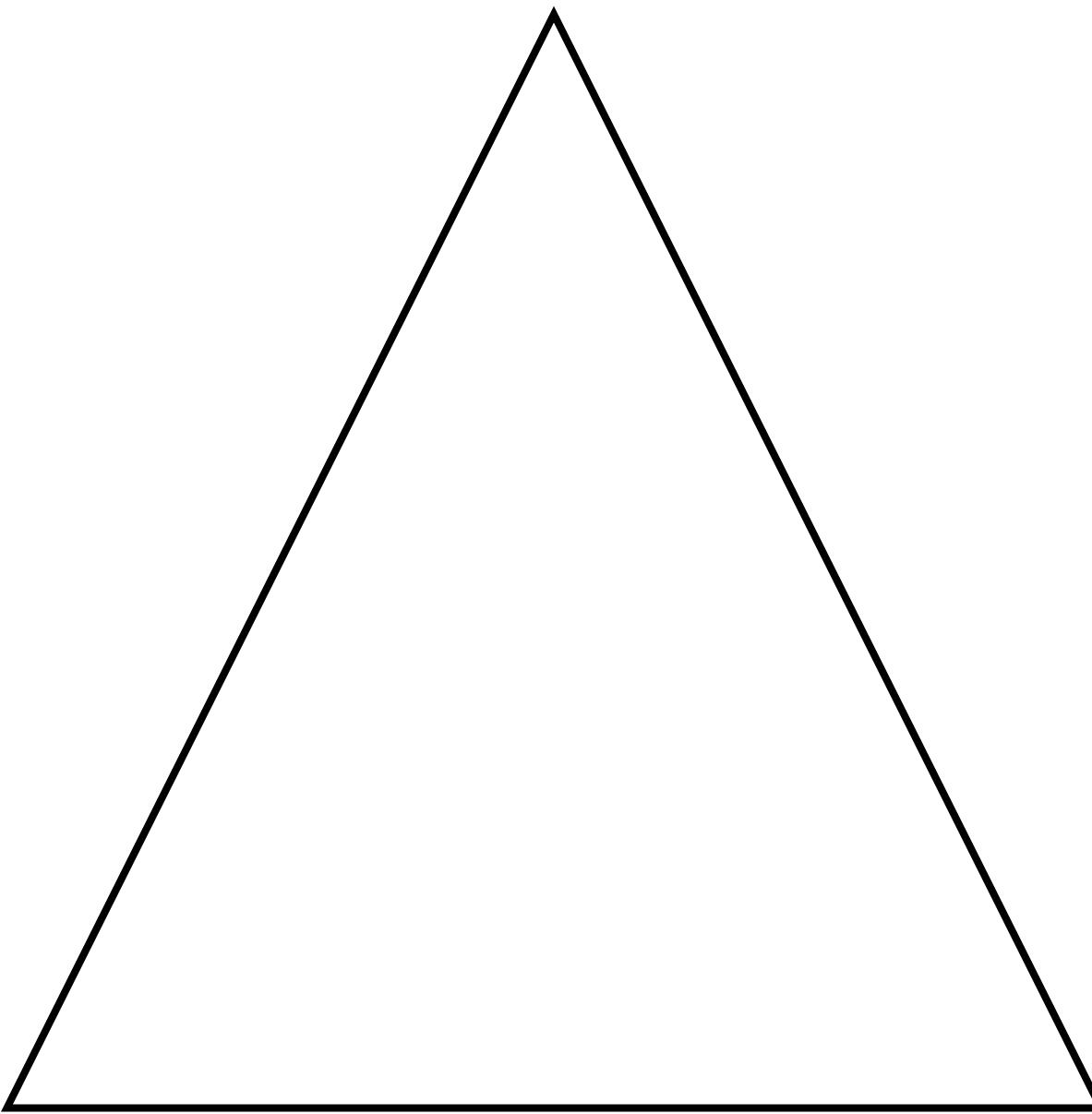
	Who can define your identity?	Reason to trust?	Usable?
CT	Governments, CAs	Almost none	Yes
KT	Key Server, app developer	Server: None App dev: maybe you'll find a good one	Yes
CONIKS	If correctly implemented, server can only censor, not define	TOFU-based, though gossip questionable	Yes
SCP	Probably a cartel	Maybe it will be a good cartel?	(?) Probably
DPKI	Your chosen delegates, and depends on chosen namespace consensus (and hackers)	Control in hands of end-user	Yes

DCS  **Triangle**

+

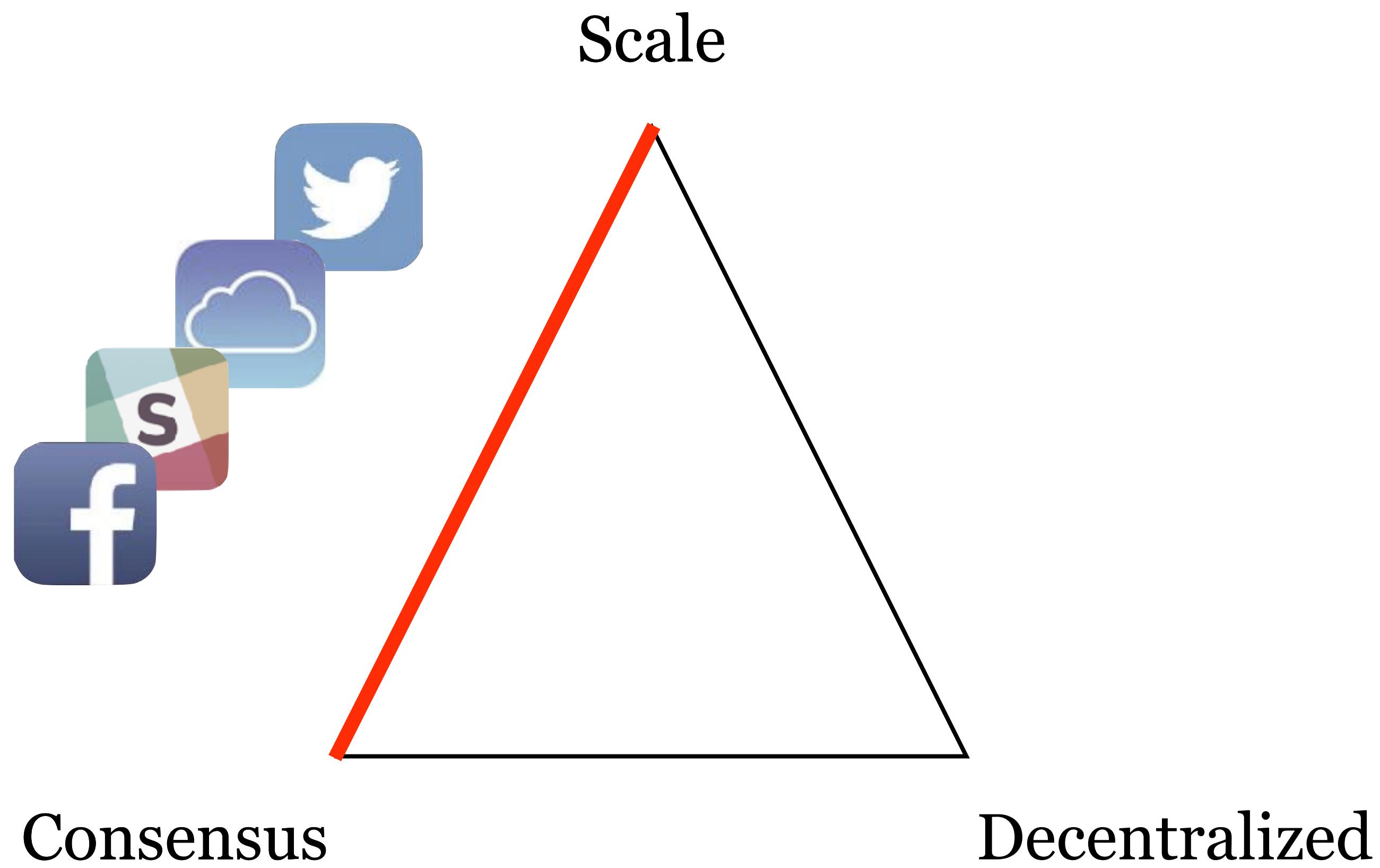
DCS  **Theorem**

Scale

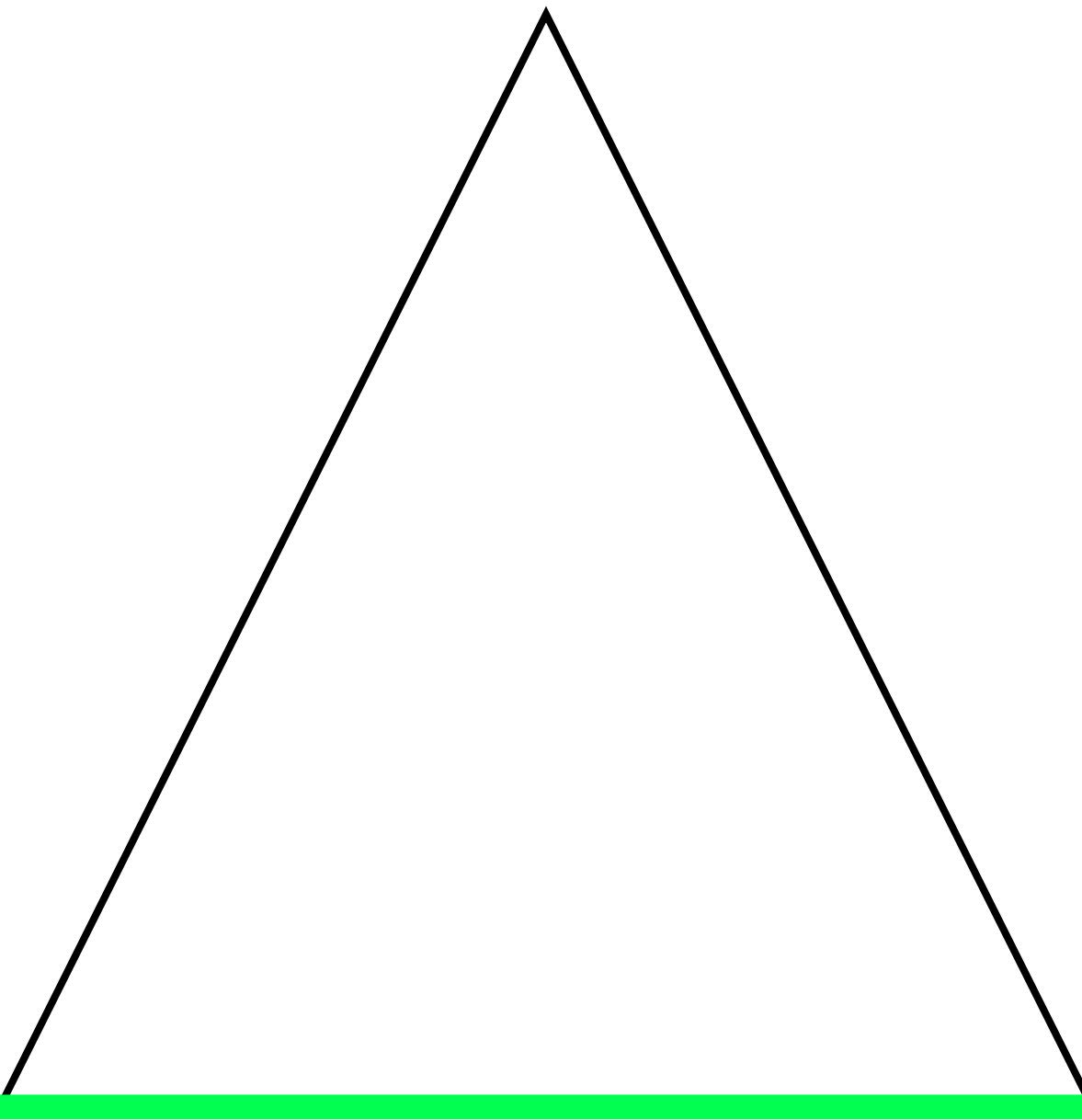


Consensus

Decentralized



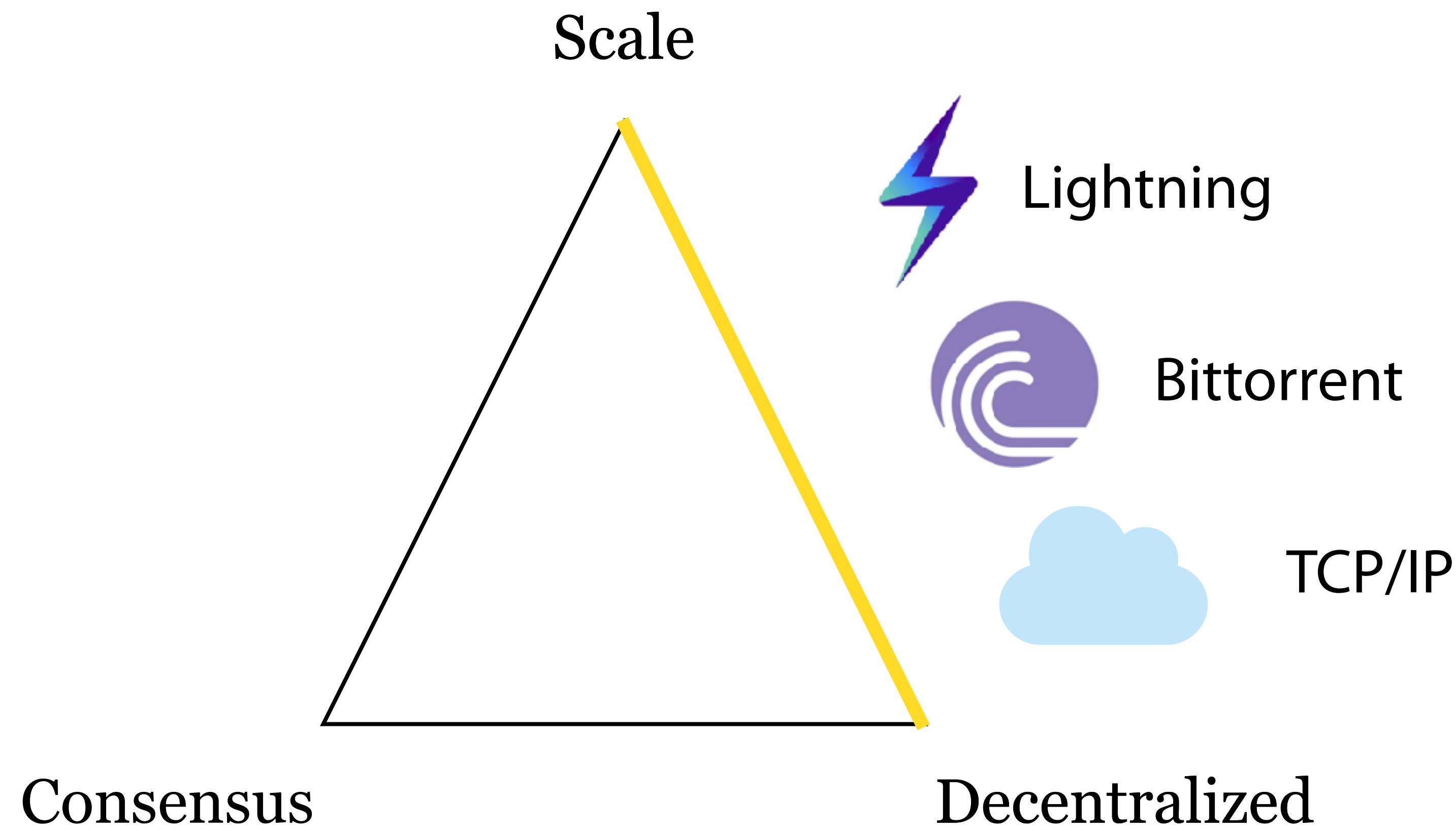
Scale

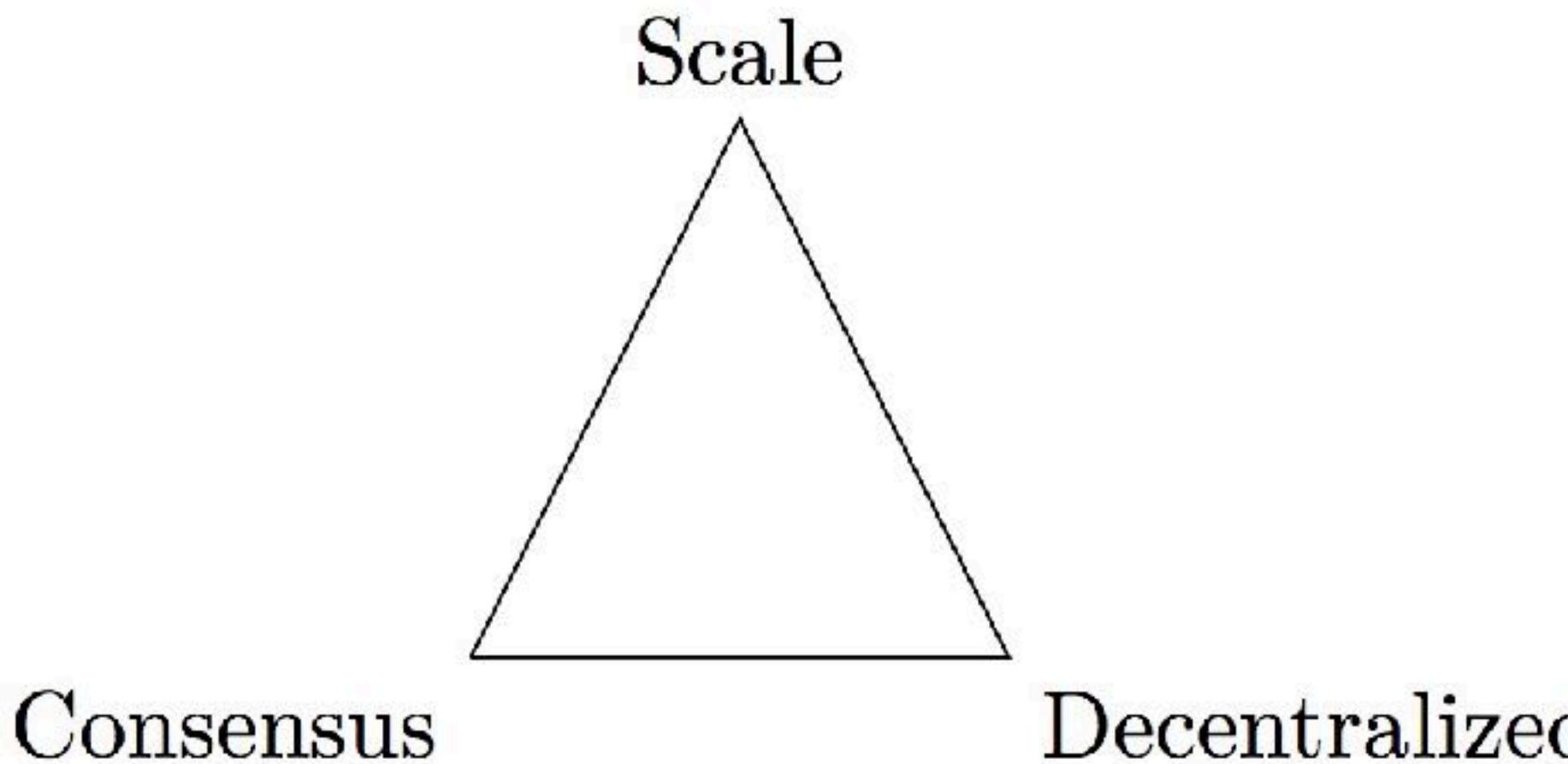


Consensus

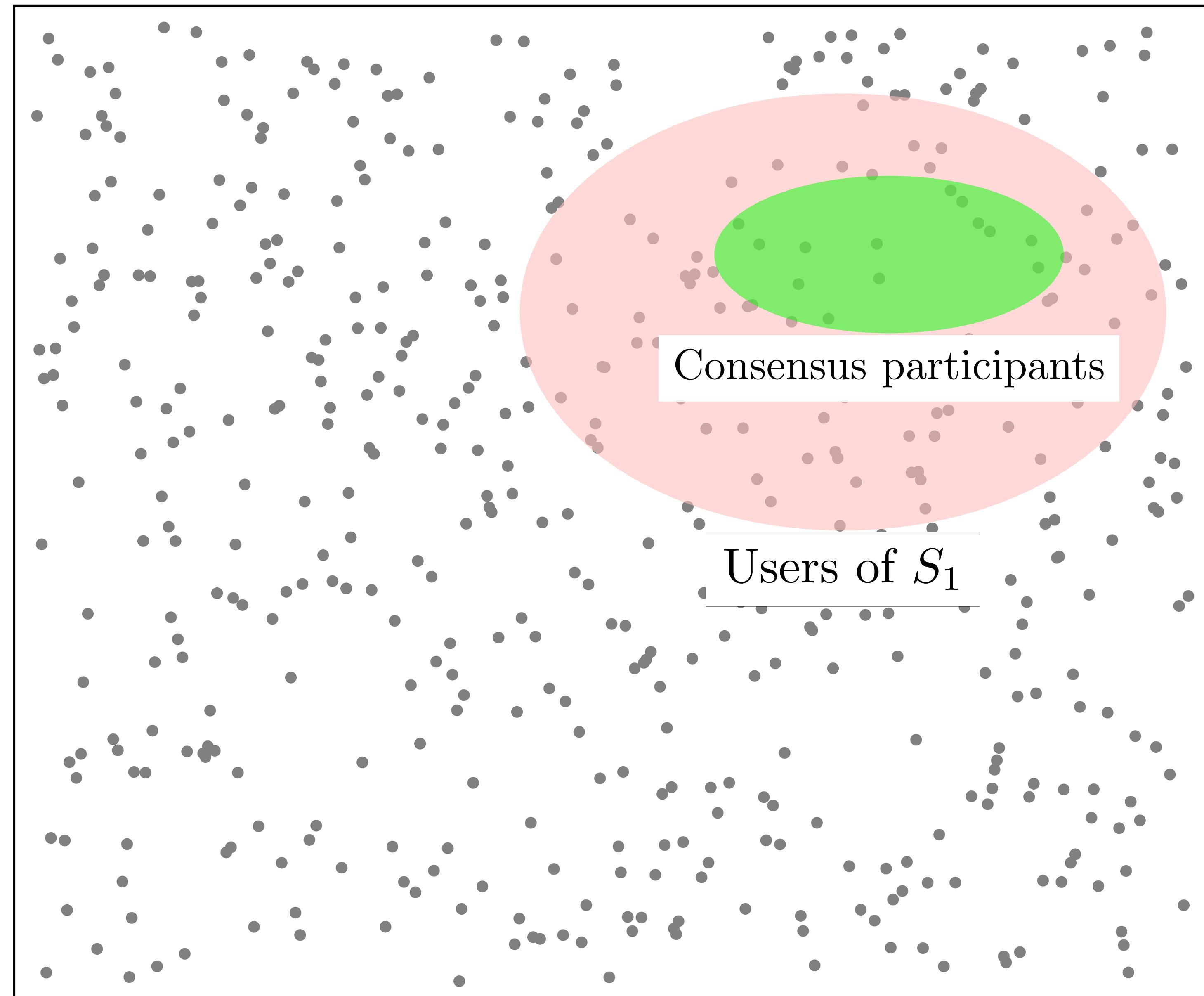
Decentralized



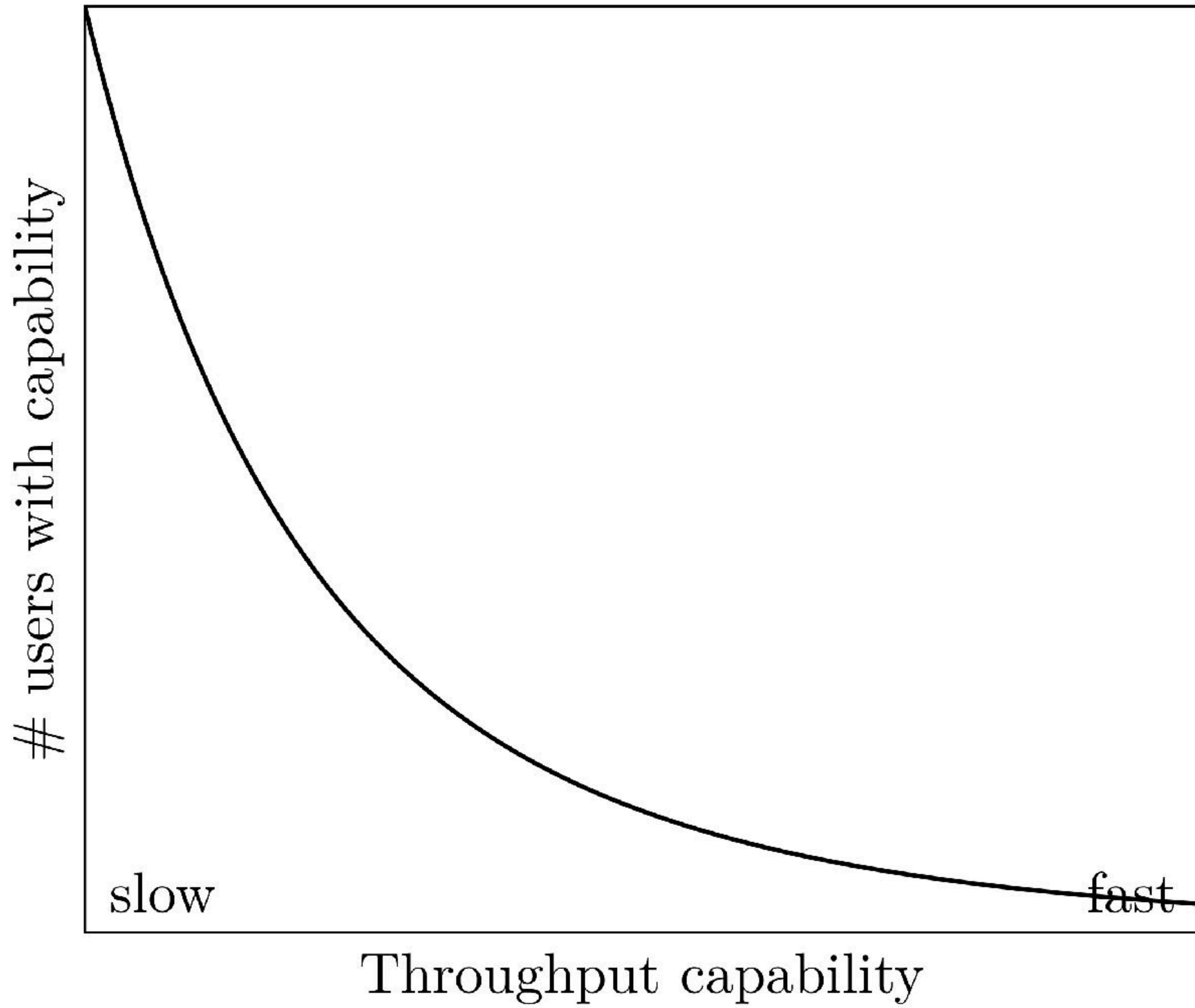


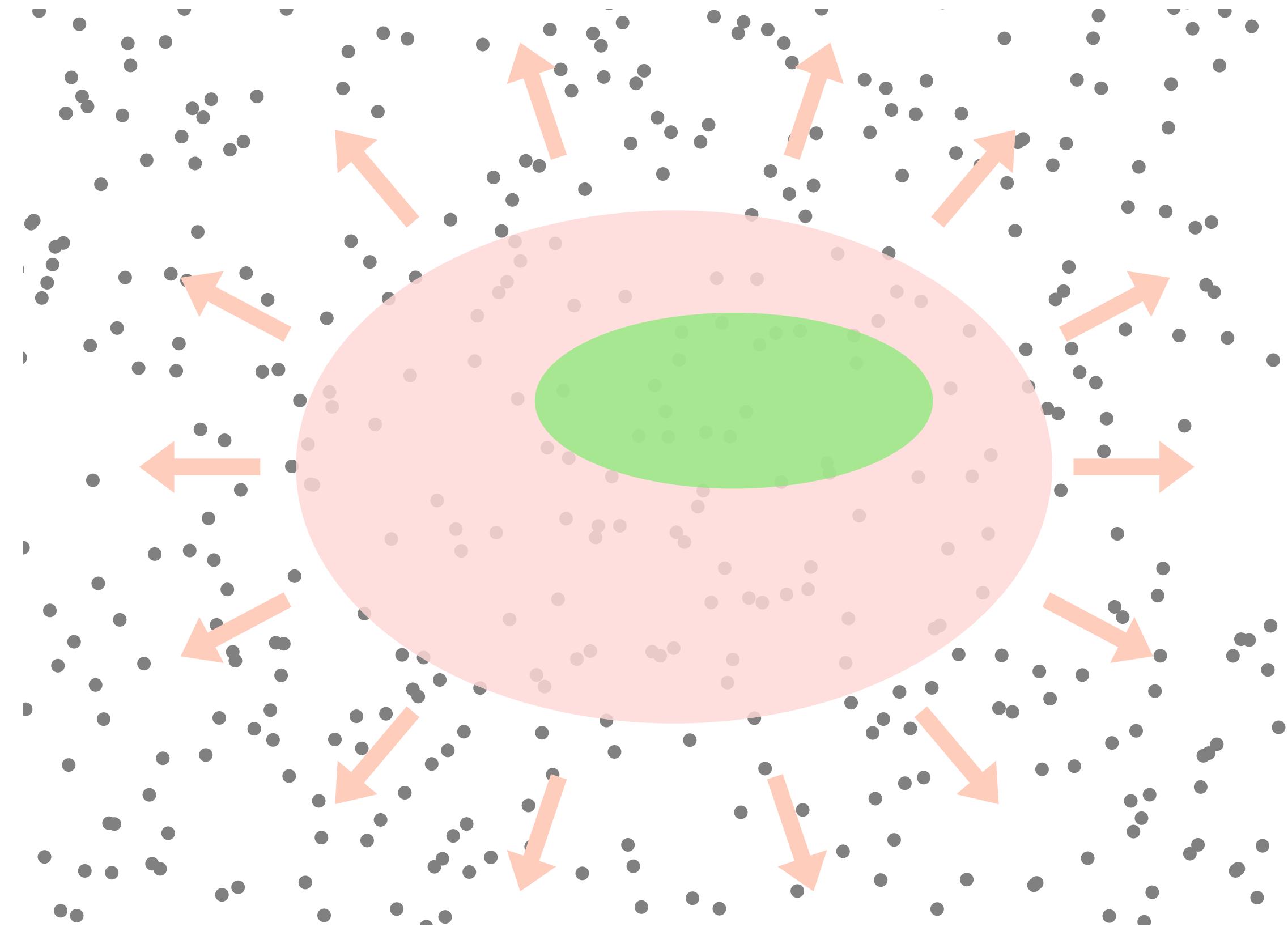
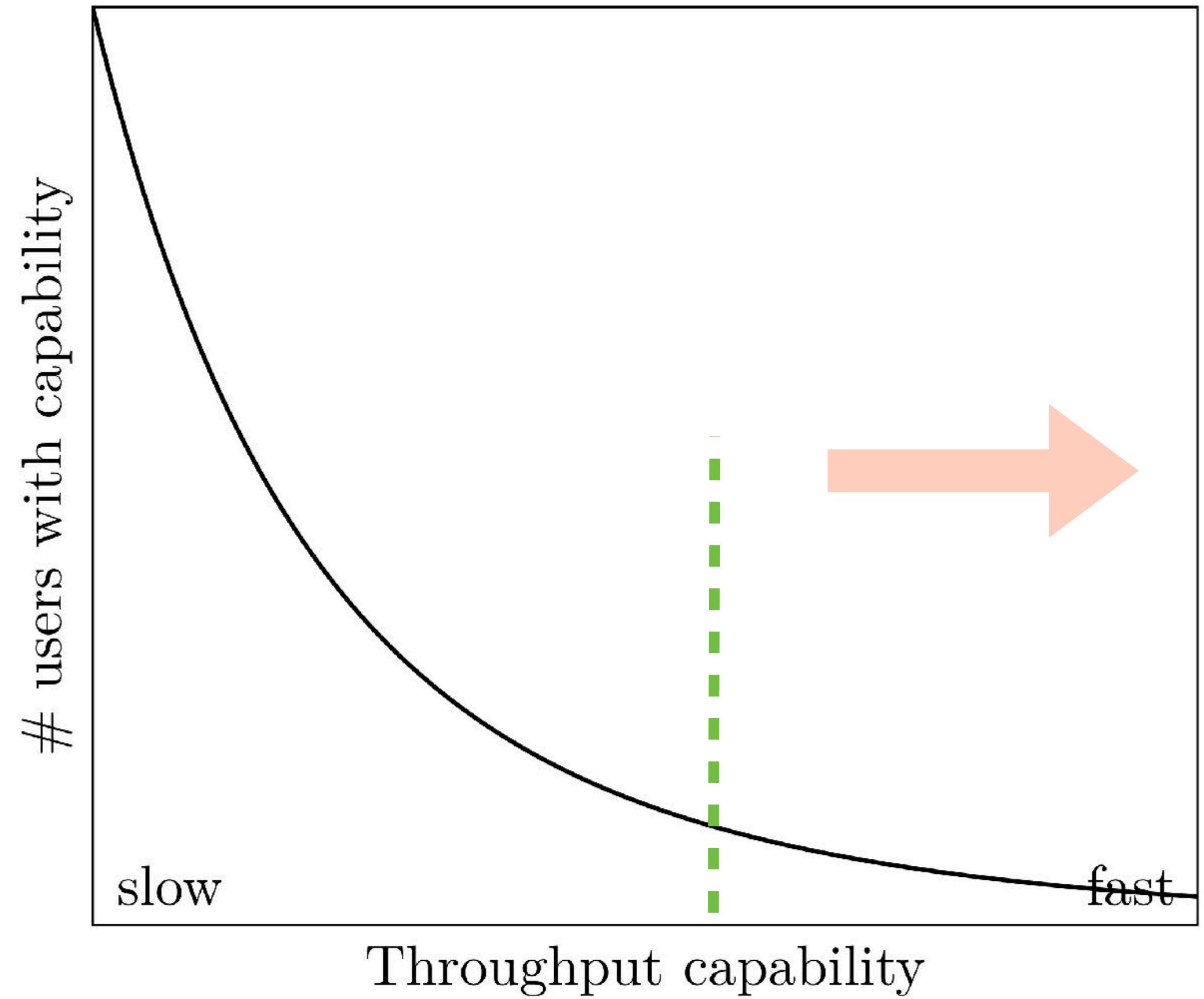


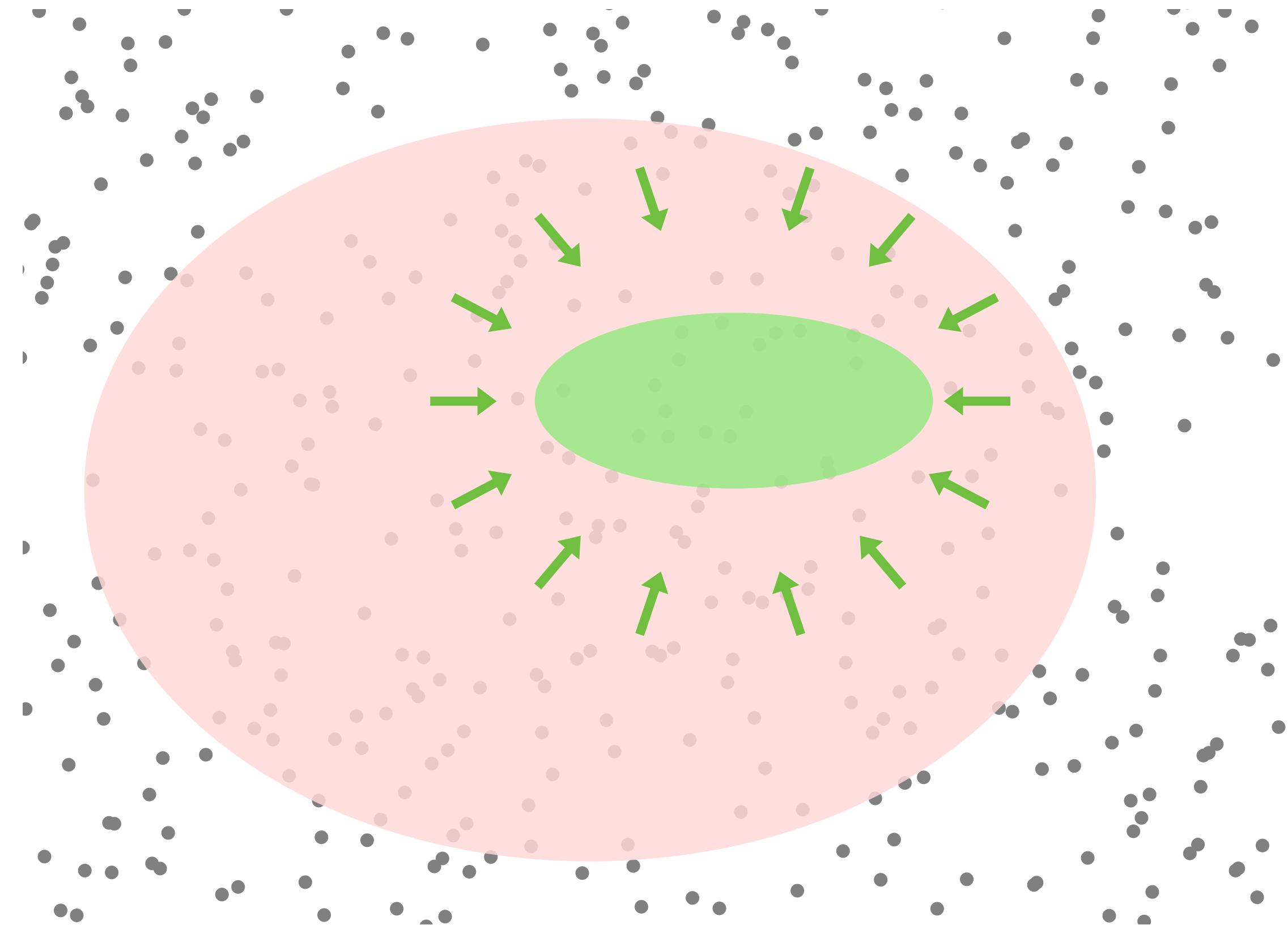
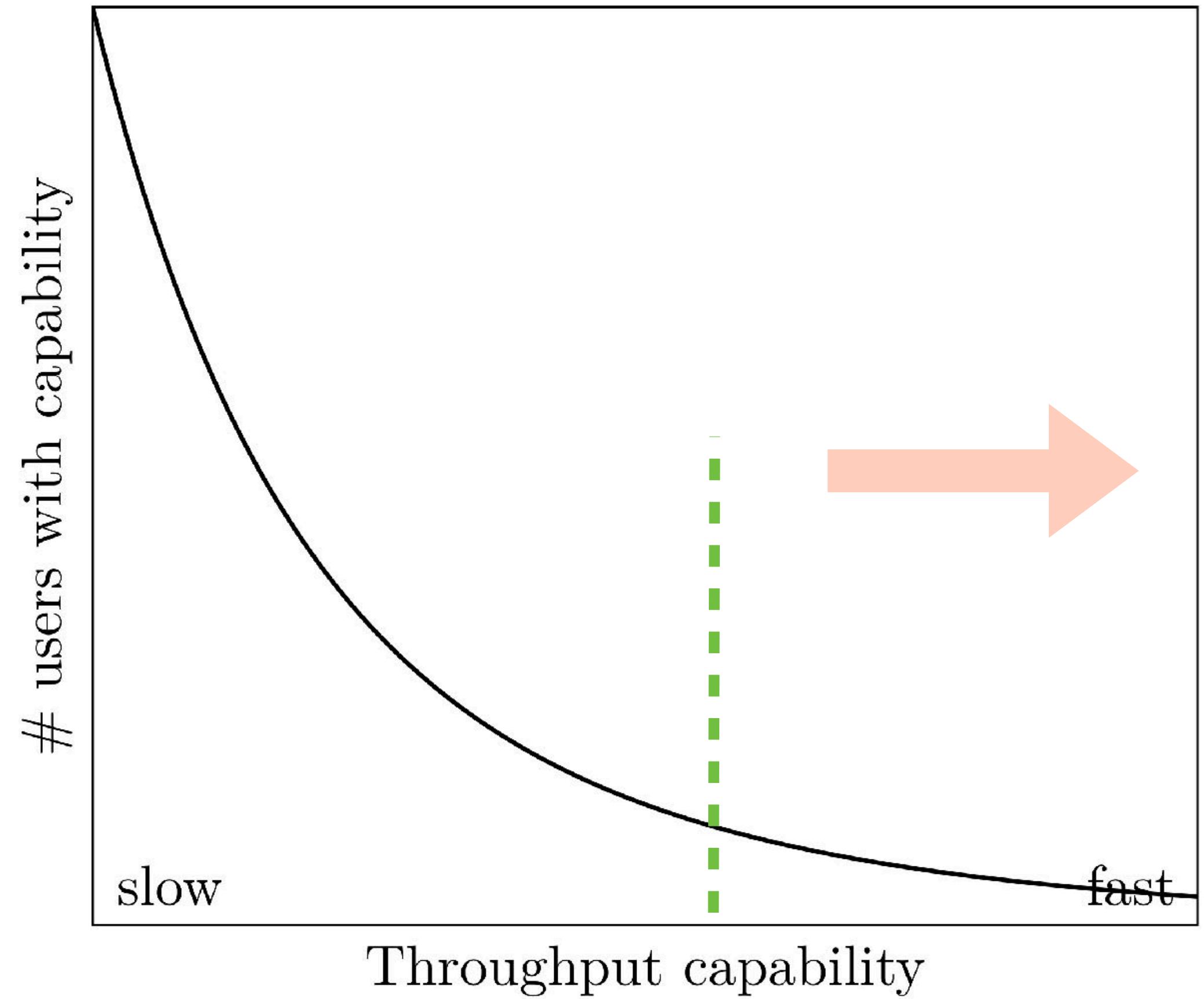
- **Consensus** means the system's state, s is a *shared state* that is updated by nodes running a *consensus algorithm* over a network, and that furthermore, the output of *consensus algorithm* determines the network's accepted output of f_S , and whether or not f_S completes within S_τ .
- **Scale** means the system is capable of handling the transactional demands of any competing system providing the same service to the same arbitrary set of users across the globe (“*at scale*”).¹
- **Decentralized** means the system has no *single point of failure or control* (SPoF). Another way to state this is: the system continues to perform its intended behavior if any single element is removed from $\{S\}$, and no single component in $\{S\}$ has the power to redefine f_S on its own.

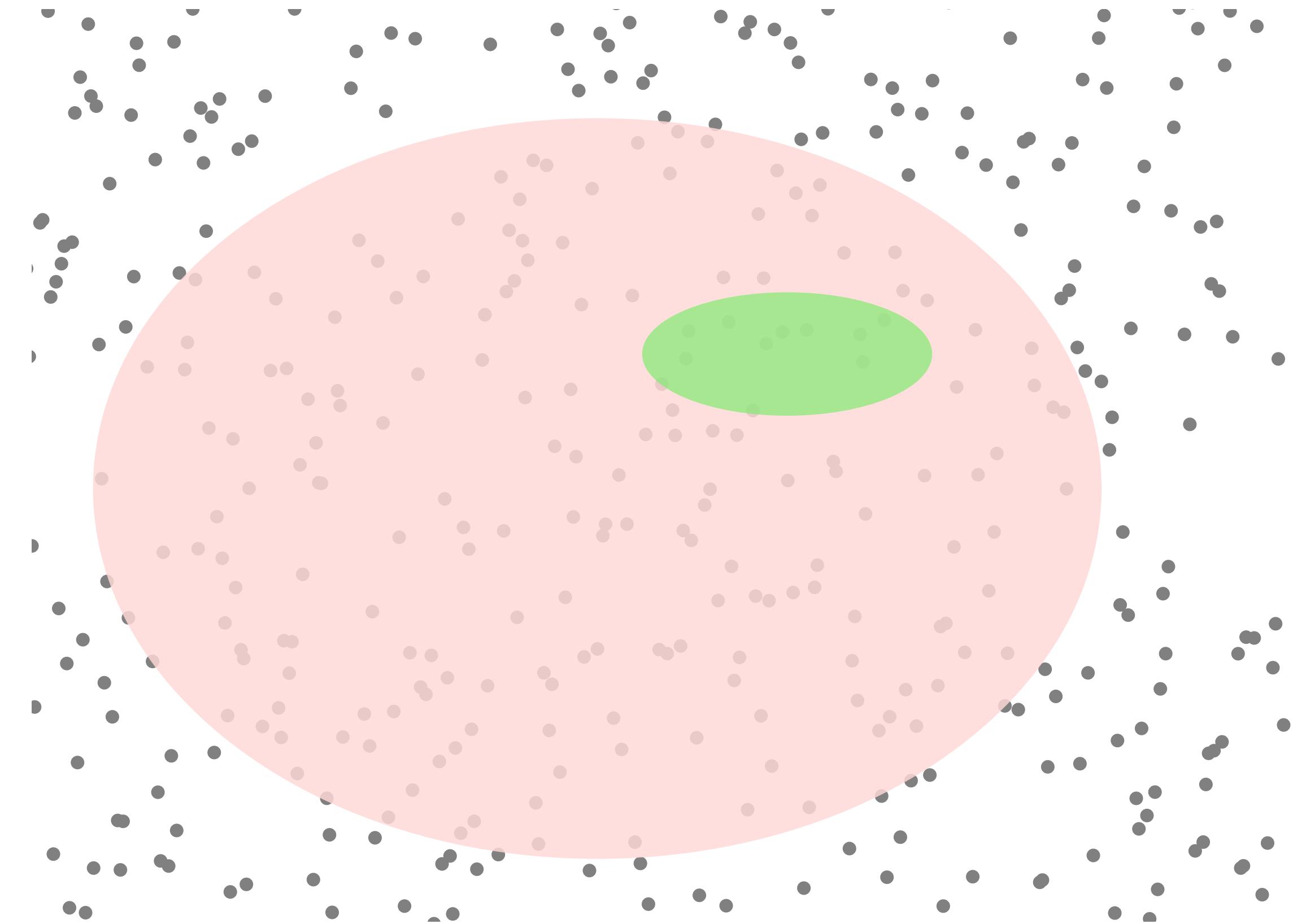
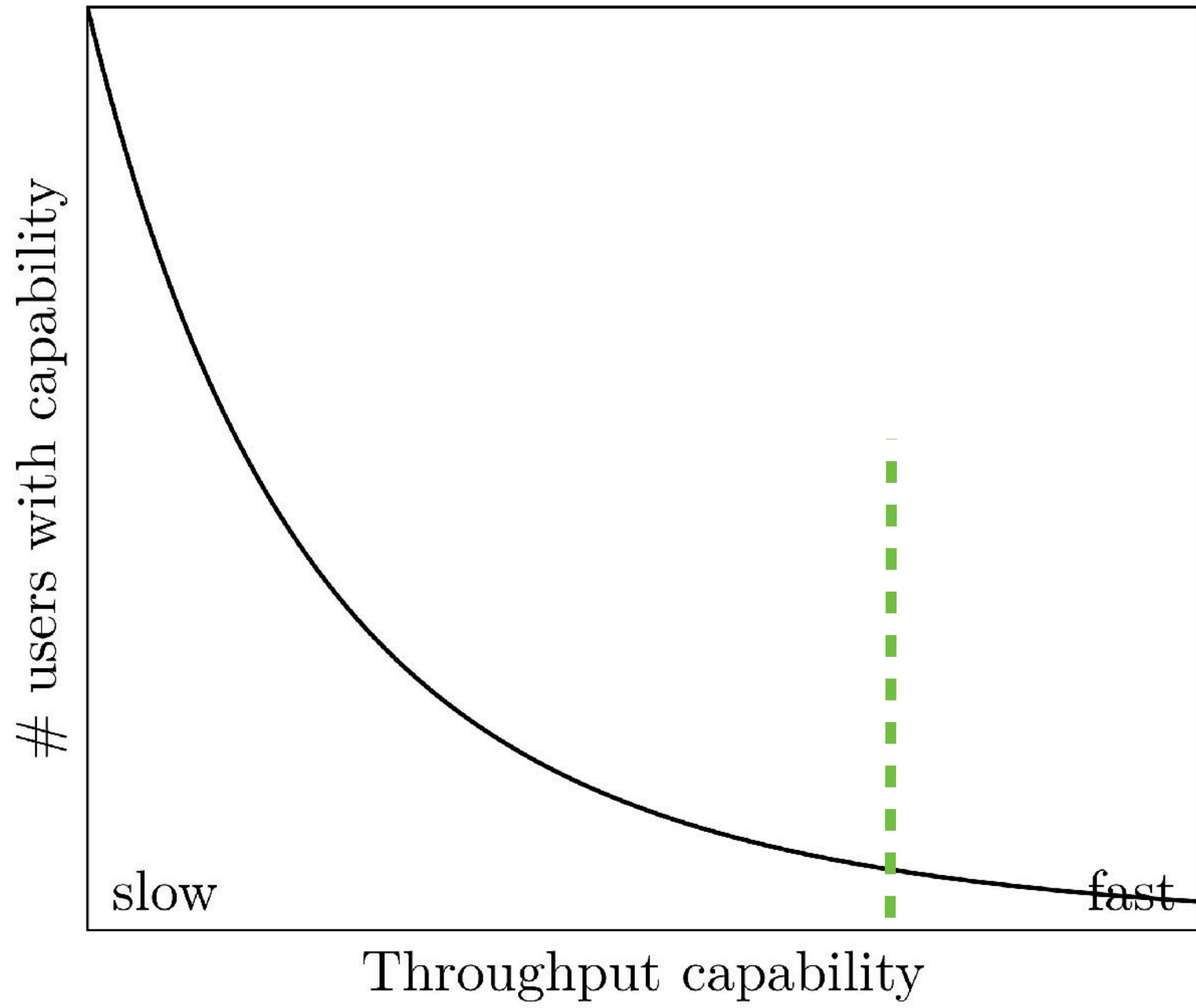


Population of users



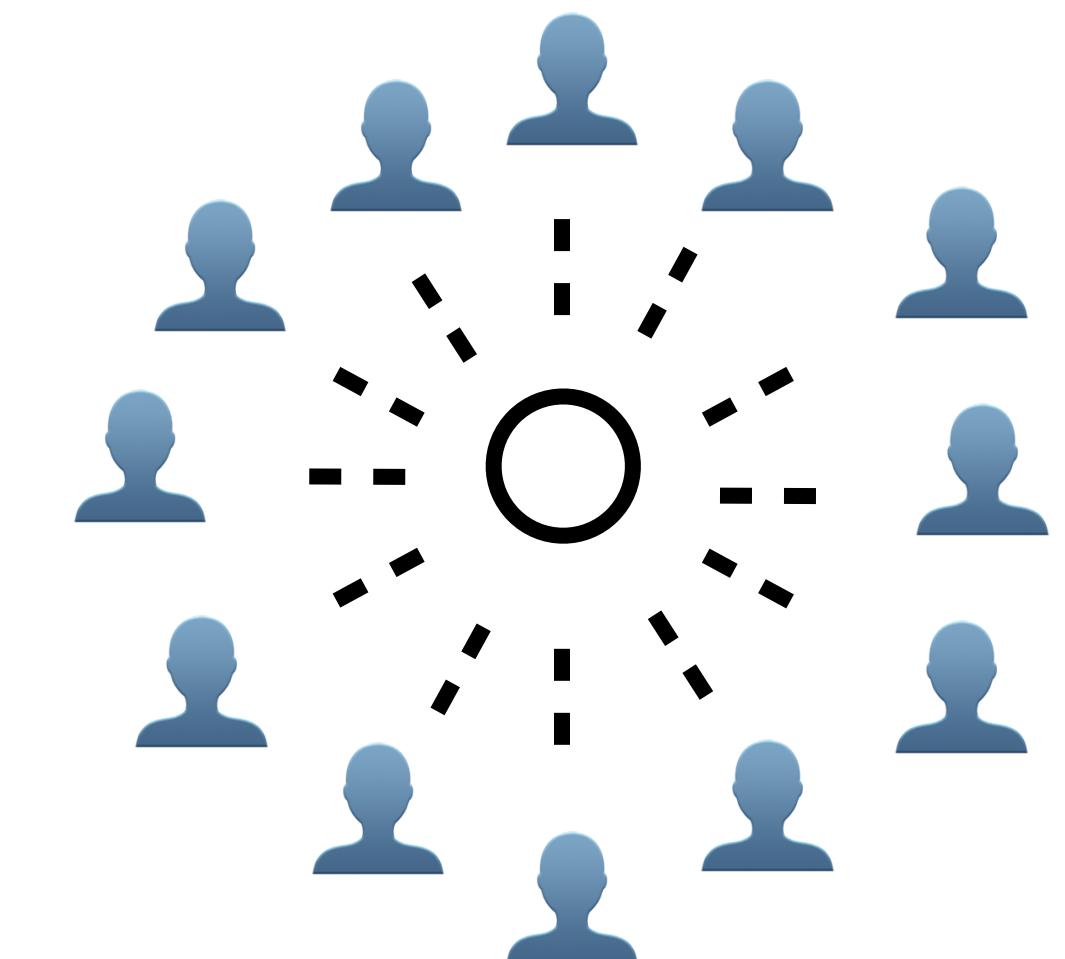
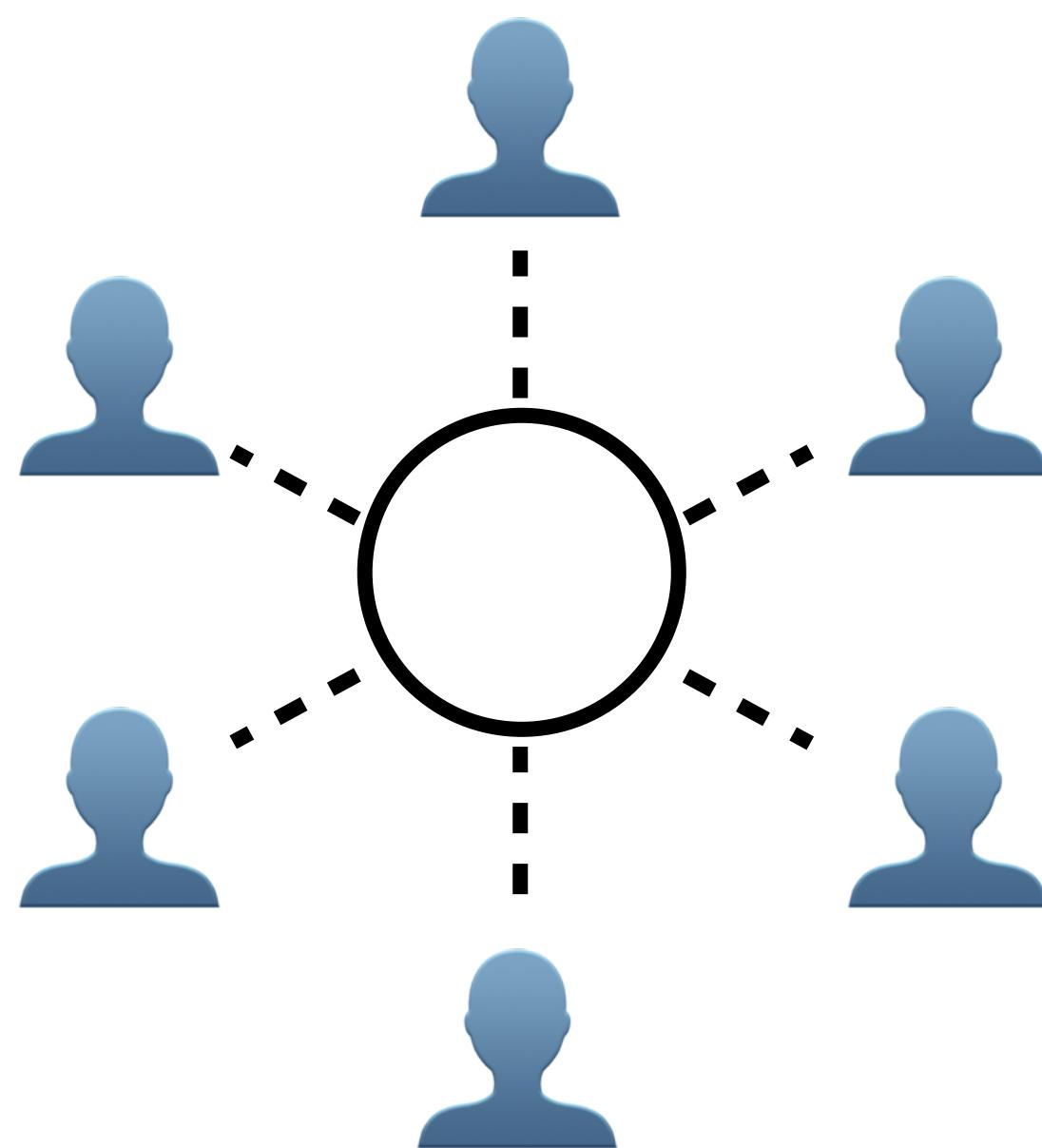
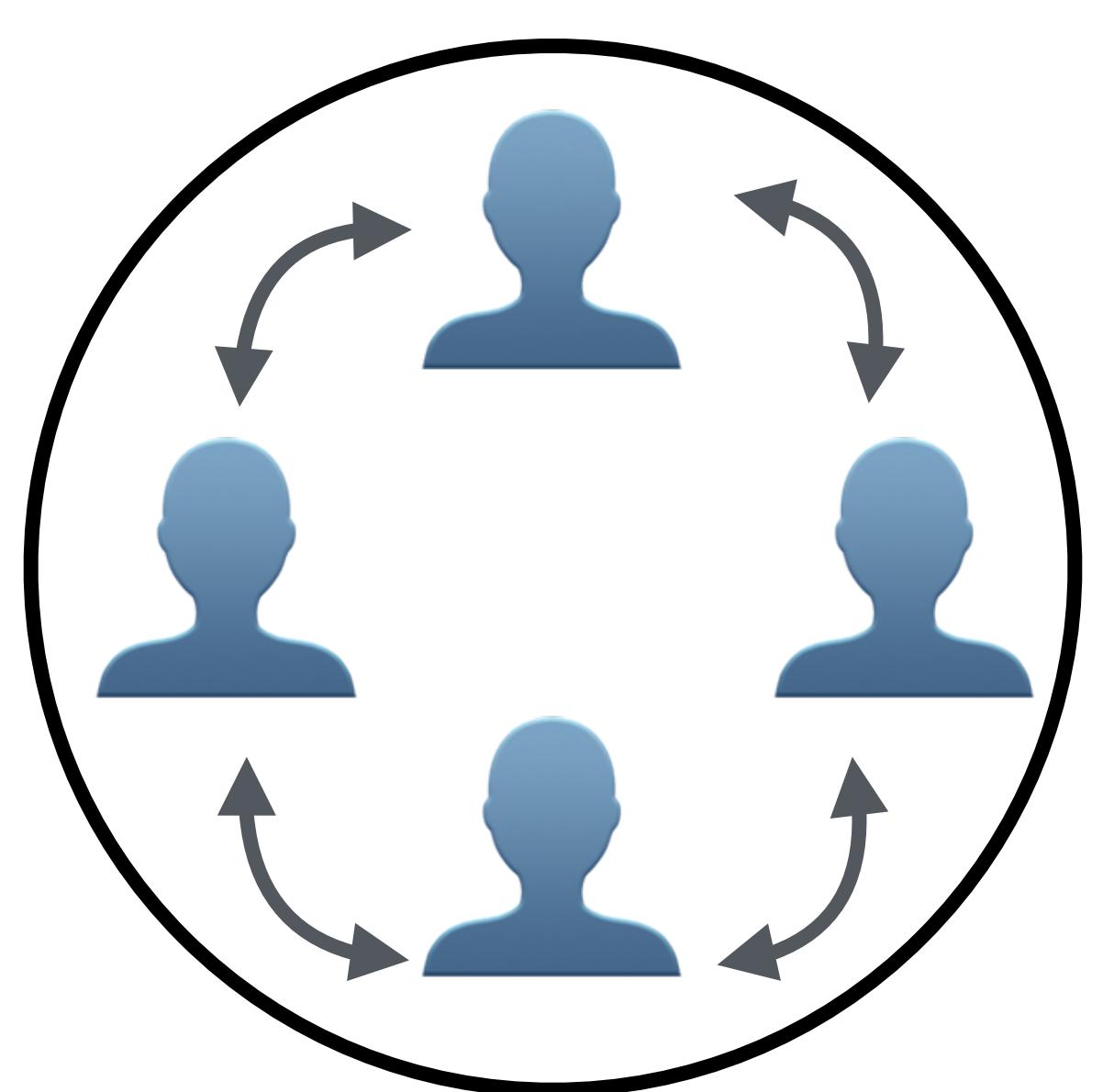


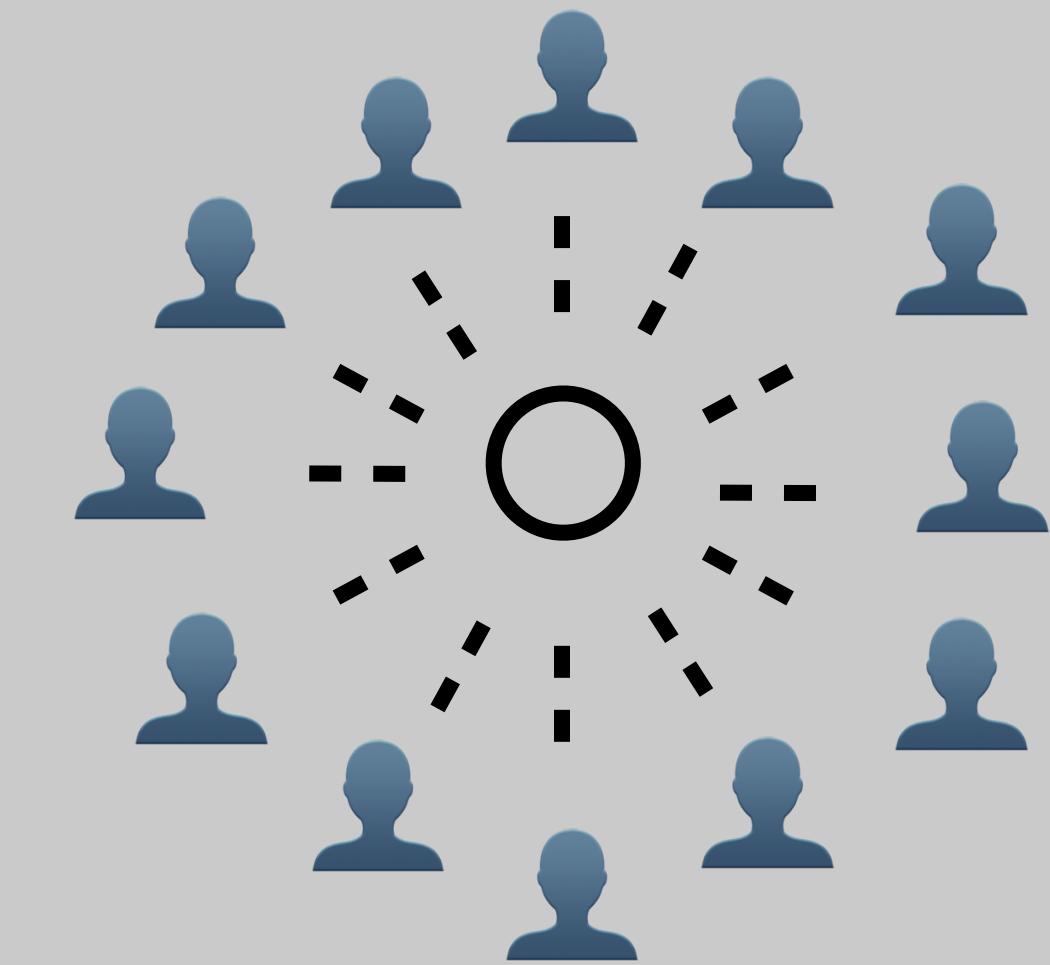
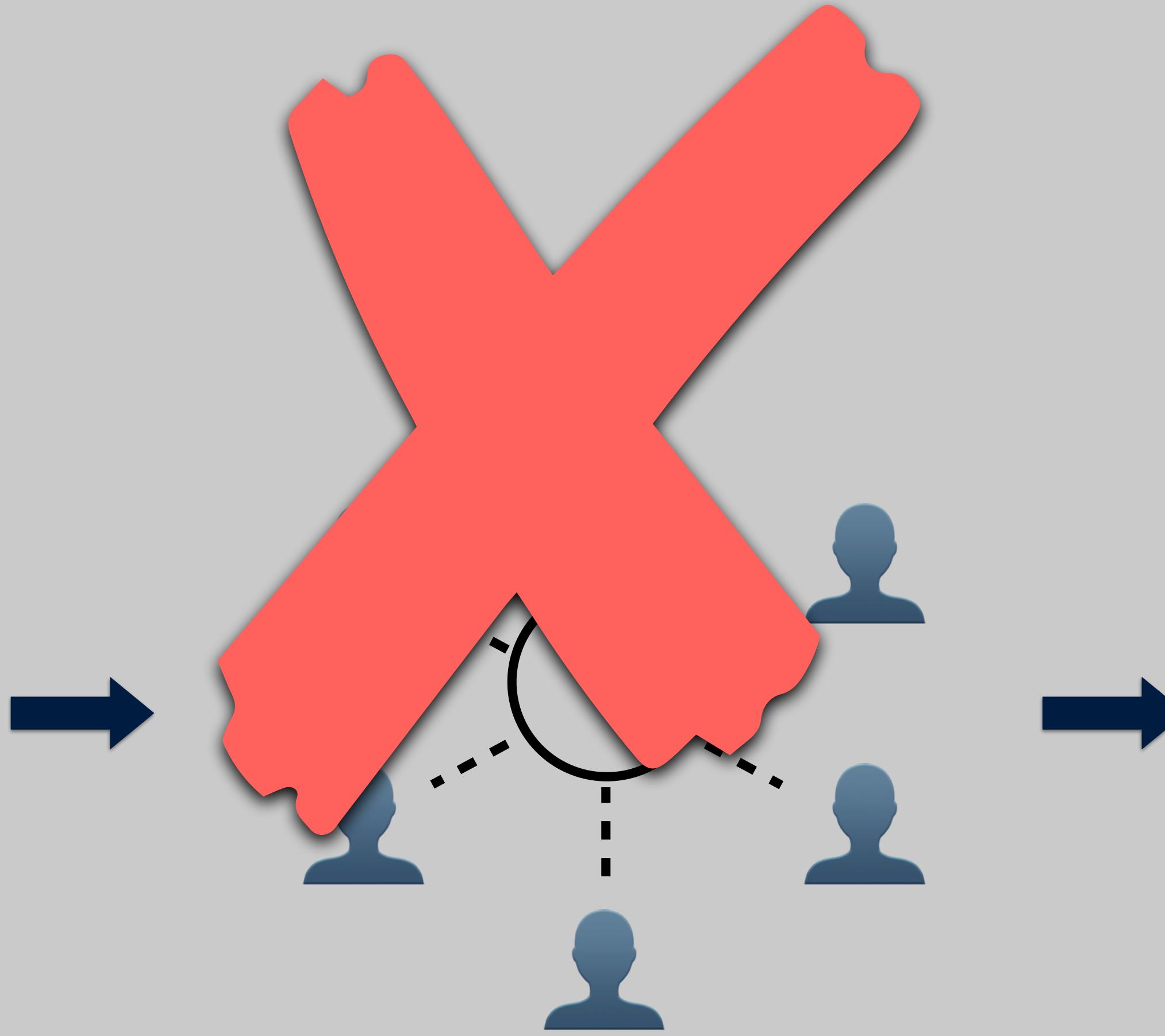
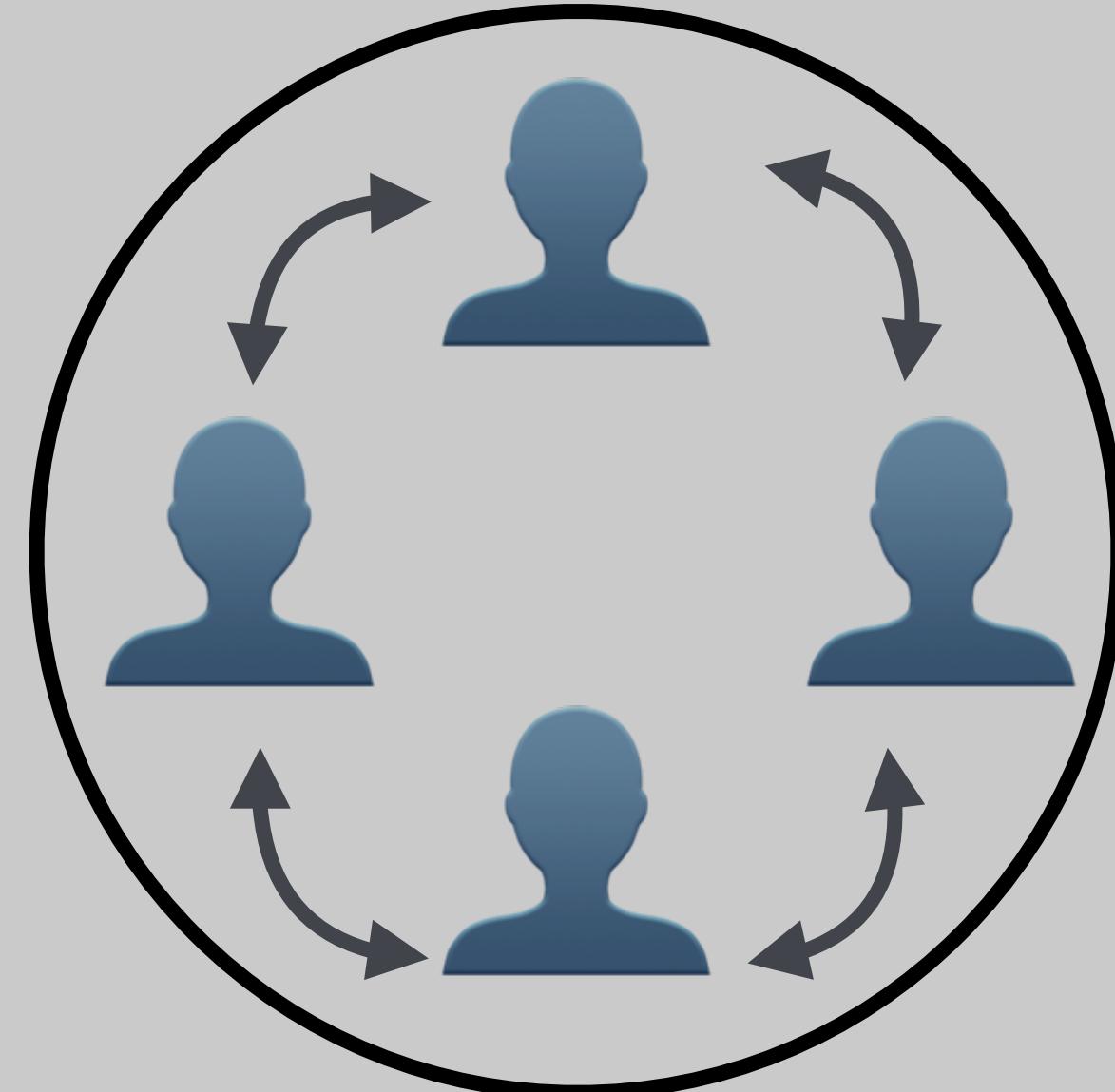




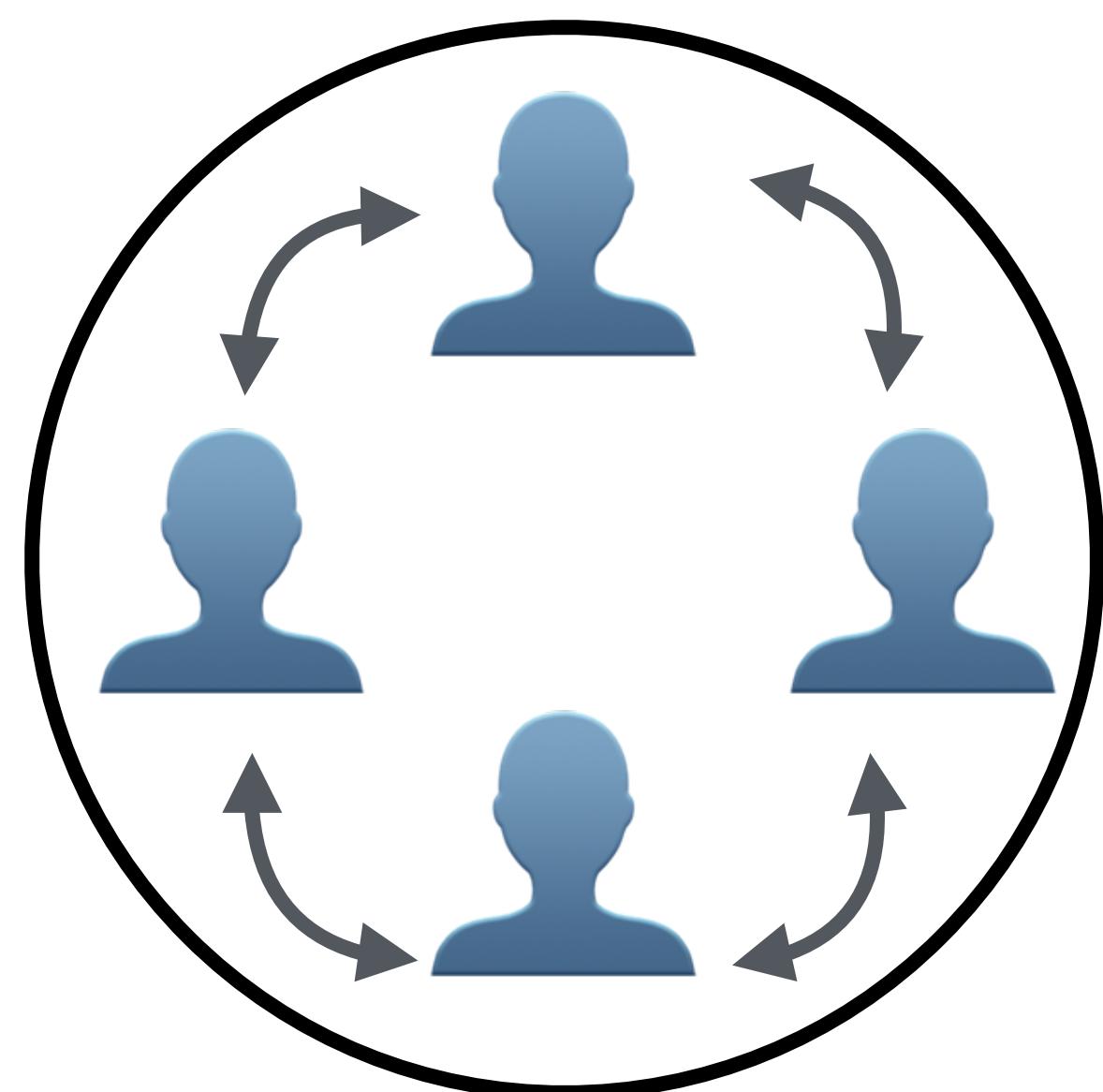
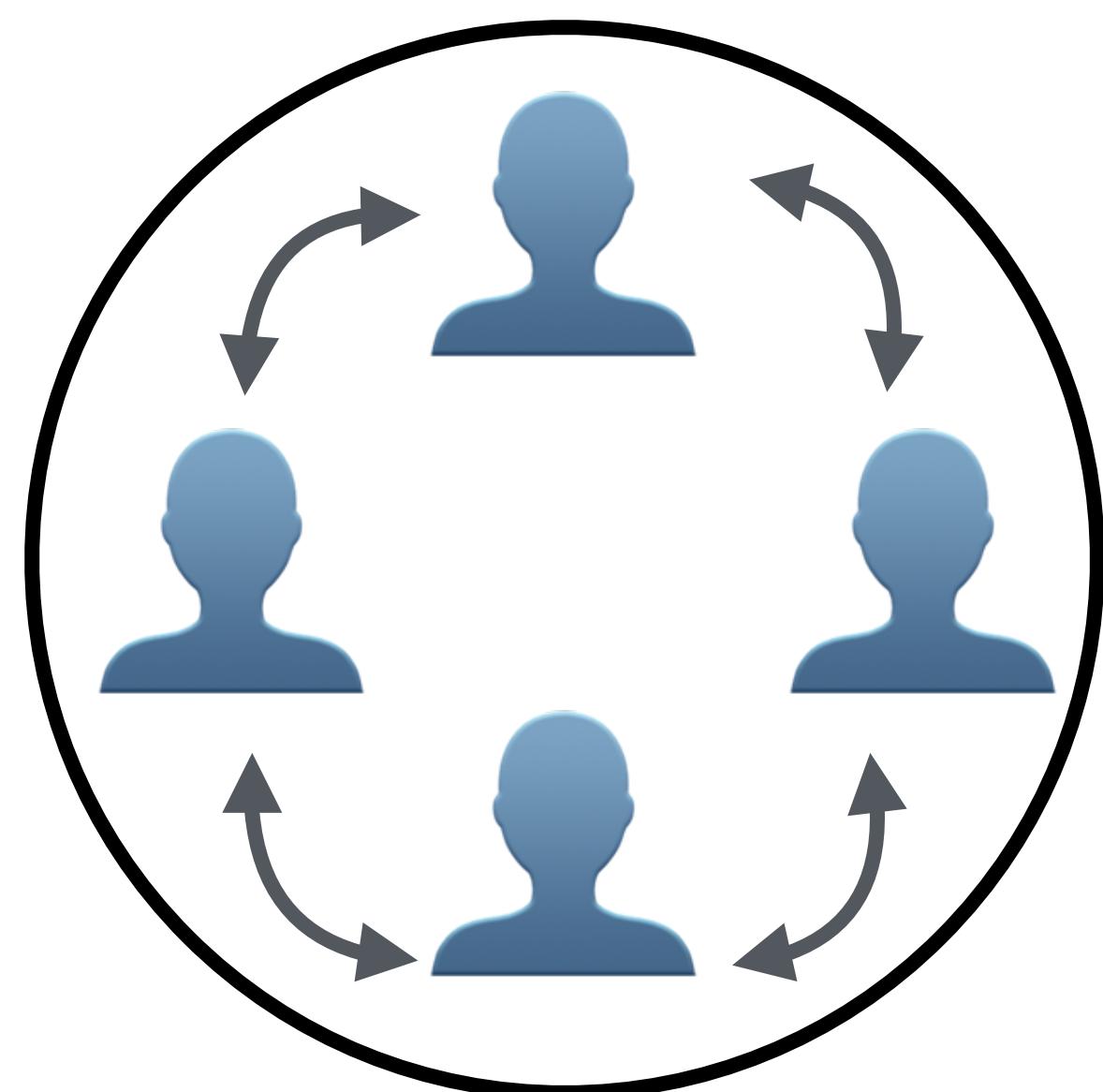
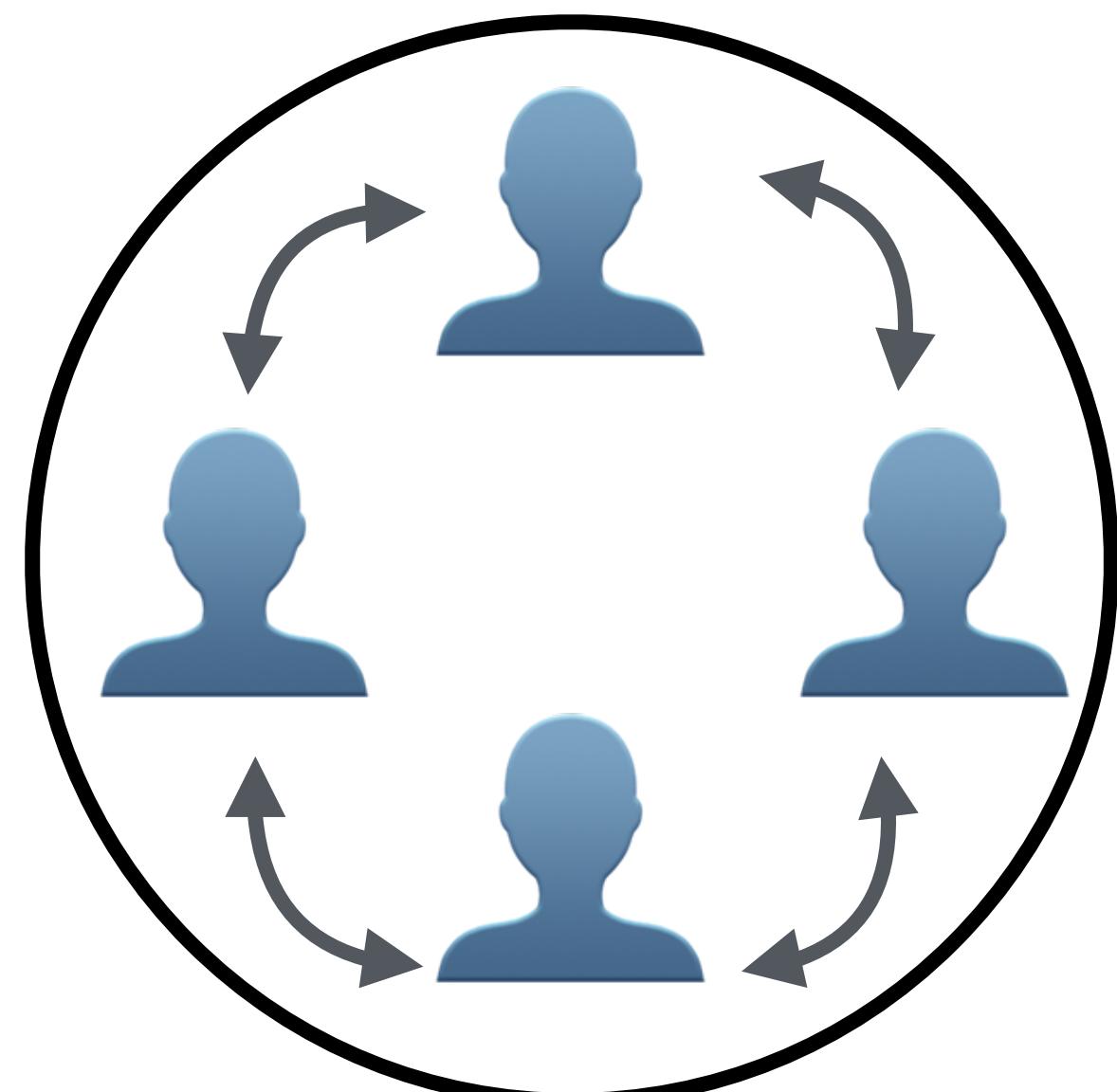
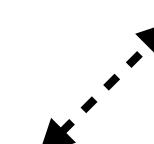
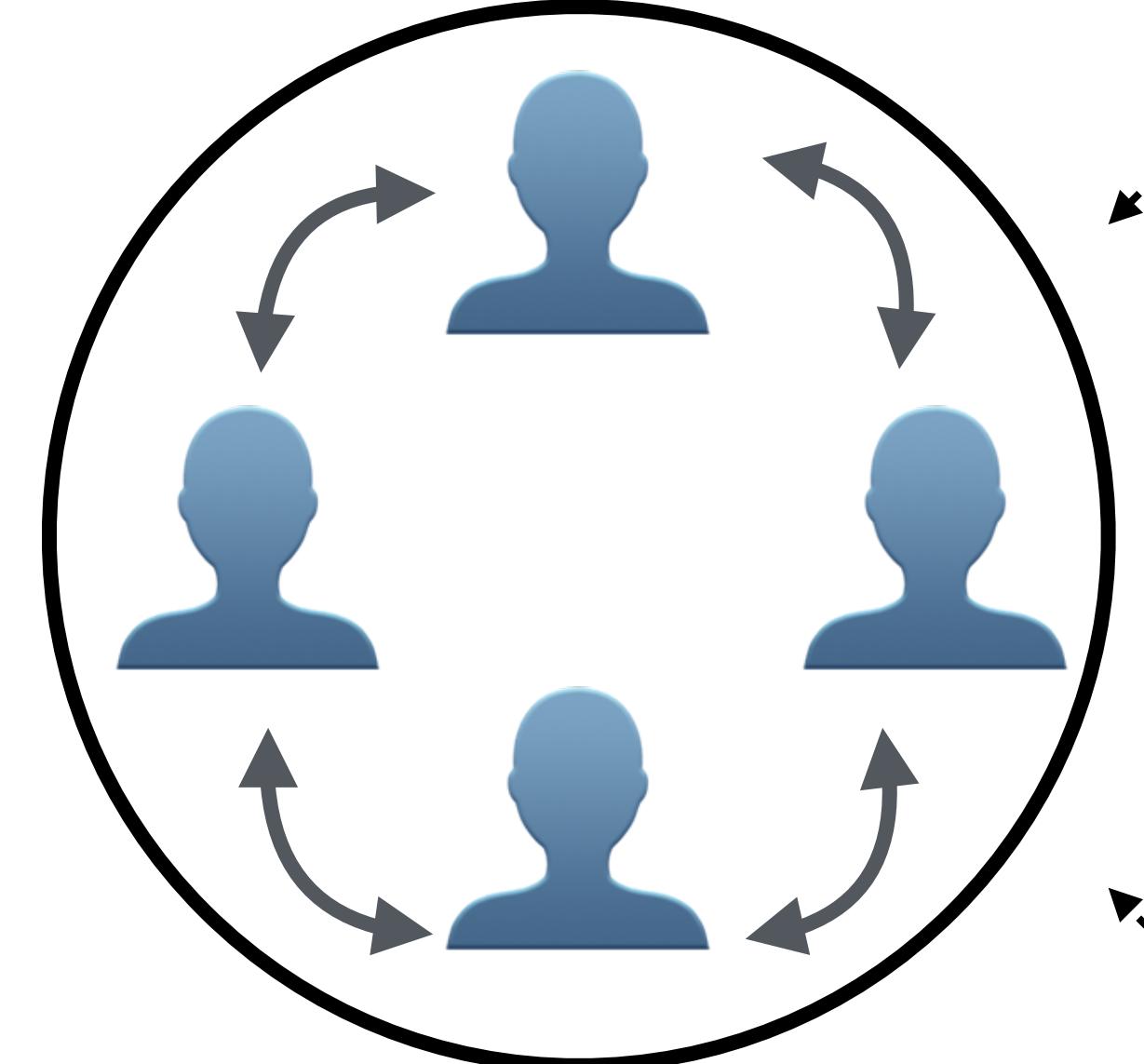
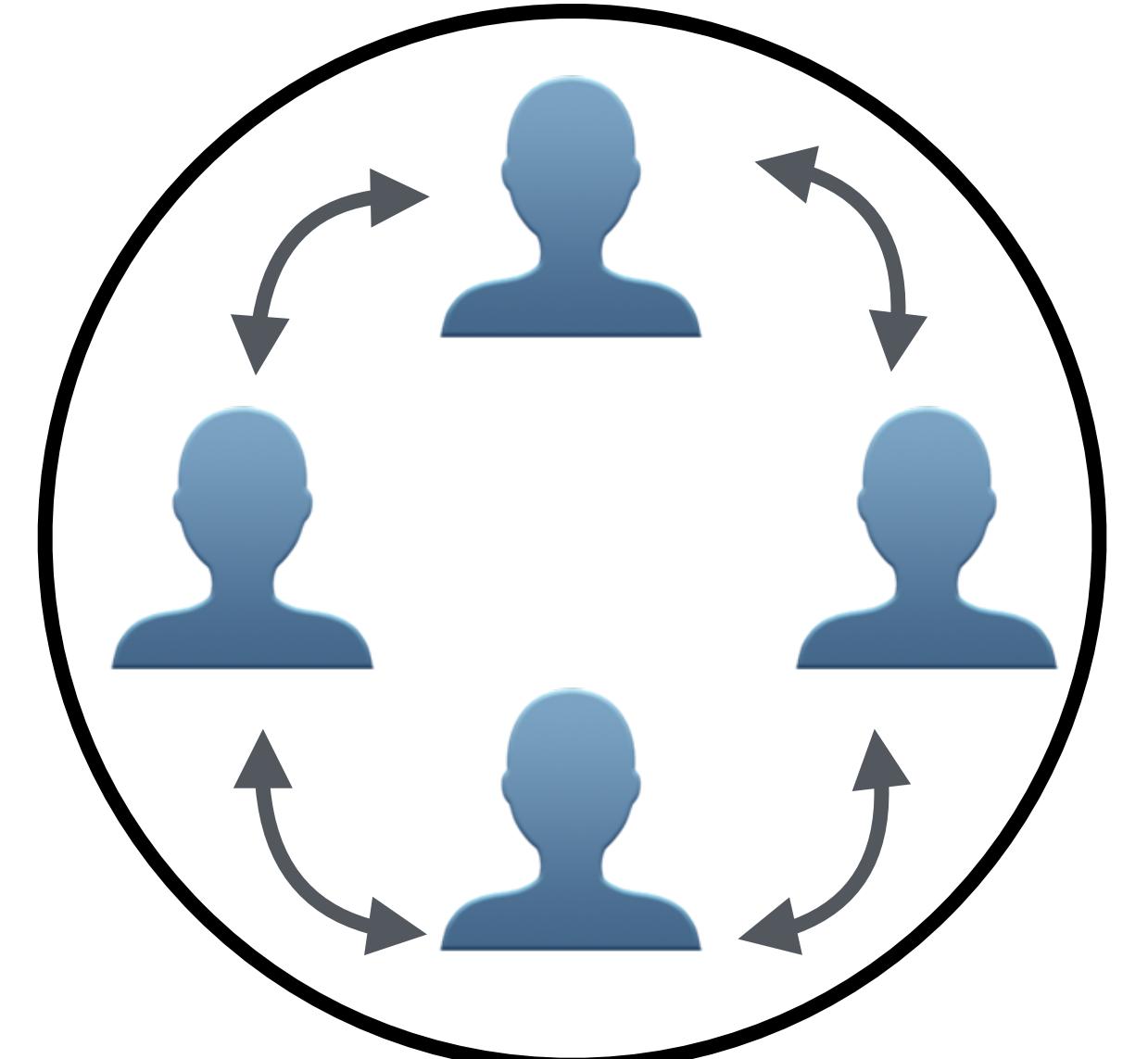
Getting around the

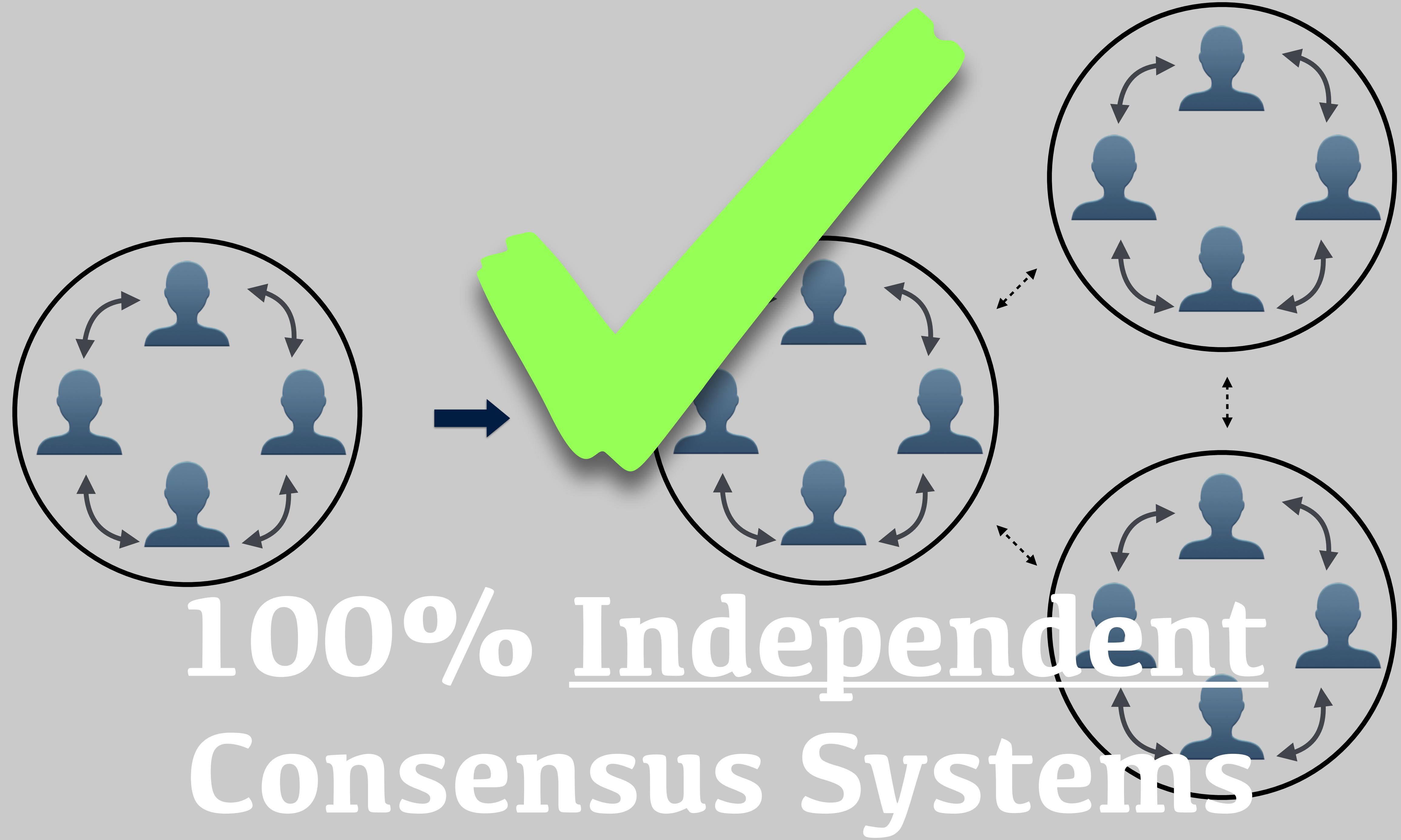
DCS △ Triangle





CENTRALIZATION!





REBOOTING the WEB of TRUST



OCTOBER 3-5, CAMBRIDGE, BOSTON, MA, USA











IDENTITY & PRIVACY IN 2025

- More and more IDs than humans
- Identity is becoming a commodity. It's the currency of commerce (see the Internet)
- Government IDs will be the best way to verify who you are
- More and more IDs mean more and more IDs

Meaning of Identity? The question is (tech, identity)
Identity exists and what problems are we trying to solve with Tech?

Goal: Improve Authentication (?)

- Logging in
- Register & login / Play Taxes (without SSN)

long lived database fingerprints
(using 2D as "finger" & from 3rd party source)

People "use" for identity today (before)

problem class "identity" solved (best, reliable, private & secure)

SSN replaced by database fingerprints & don't reuse

users with untrusted keys (robust)

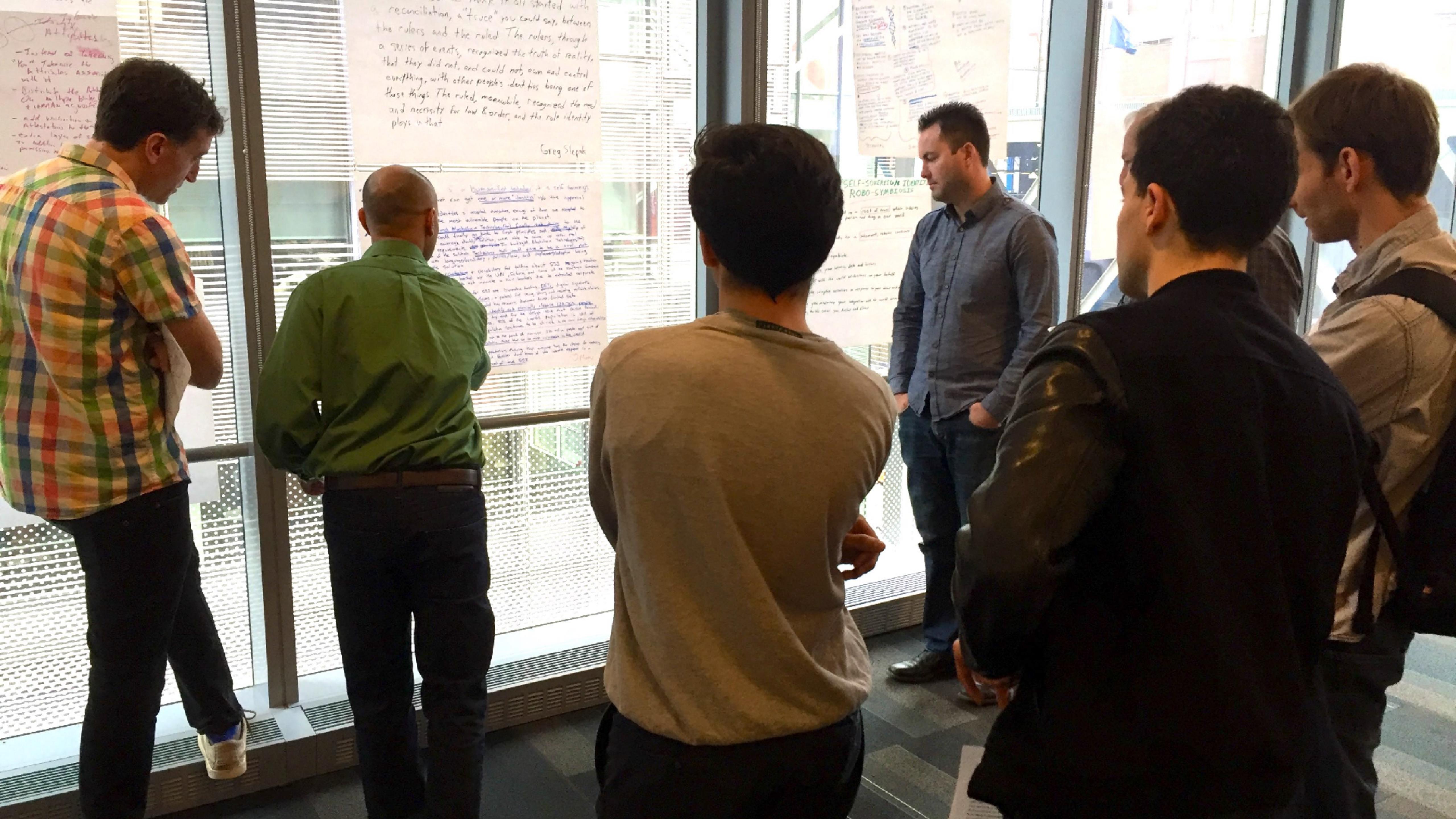
Looking back, we are
gained control over &
more flexible & more parti-
culars and automated verifications
consumers & social sources

I myself am surprised
that was both fully decentralised
surprised obfuscation of the
This required not just new so-
cial structures, rethinking of encryption as well
around detecting compromised

Progress On implementation
good governments can little need for
bad governments did not want to
bad governments identity given to
access to documented identity sought in the
to get their own systems adopted in the
change. Showing the economic gains
that this was true has helped with

-

Greg Slepak





What's **Rebooting** all about?

Works produced by **RWoT**

- **DPKI** overview and description
- **DID** Specification — Decentralized Identifiers
- **Verifiable Claims** — together with **W3C Credentials Working Group**
- Actual implementations
- And more!

Attendees are expected to stay for **all 3 days**, working with their group on their projects, and have **a real deliverable** by the end of event.

We have a great time while **Getting Stuff Done™**

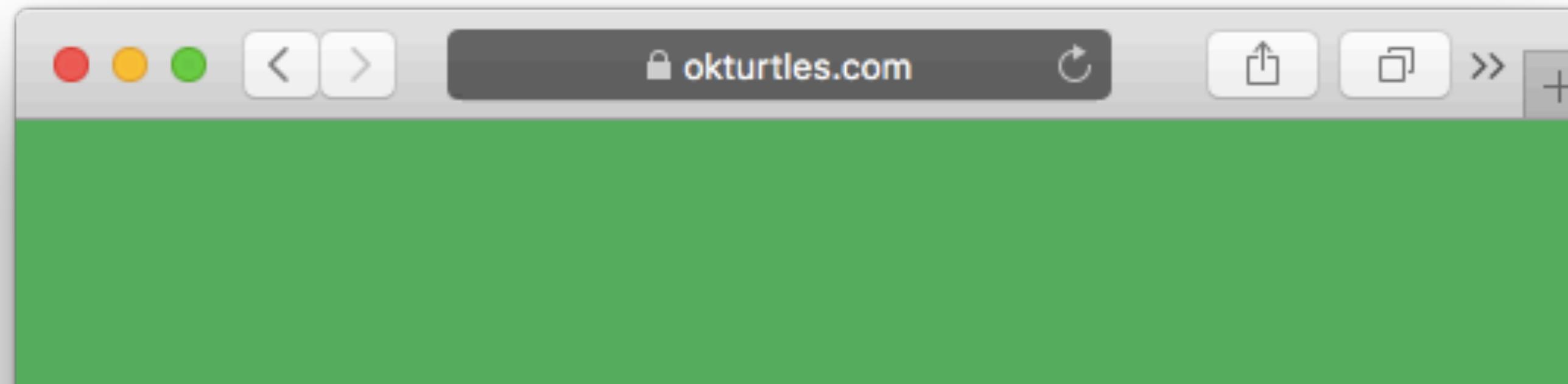
“Six companies demonstrated
DIDs and **verifiable claims**
over 2 public blockchains, 2
private blockchains, and IPFS”



Last Week at Rebooting...

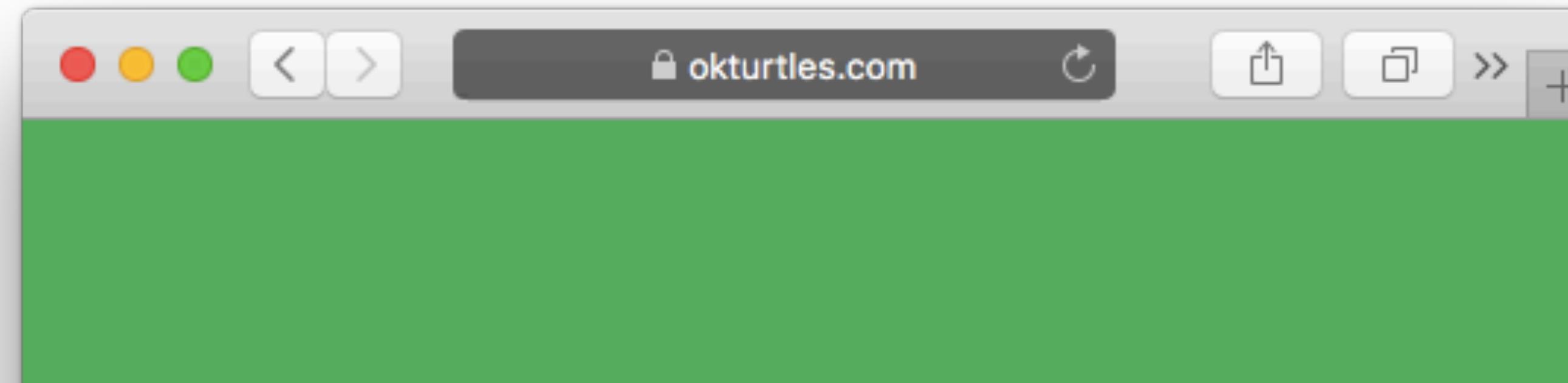
weboftrust.info

DPKI gives you reason to have
faith in the lock icon



DPKI gives you reason to have faith in the lock icon

- Only decentralized namespaces allowed
- Identity controlled by **you**
- Spec **requires** decentralization at every point to minimize trust, including lookup
- Spec **requires** private keys never be generated or stored on a server
- Your choice of consensus system



Potentially DPKI-friendly
protocols and implementations

Potentially DPKI-friendly

- **DID** — Decentralized Identifiers¹ (*Rebooting Web-of-Trust Protocol*)
- **EIP 137** — Ethereum Domain Name Service²
- **Blockstack**
- **uPort**
- ...More? Feel free to suggest!

¹ <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017>

² <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-137.md>

Contributing

- Read the DPKI paper And the DPKI issues in:
github.com/WebOfTrustInfo/rebooting-the-web-of-trust
- Attend **Rebooting Web-of-Trust** → weboftrust.info
- No need to ask for permission to contribute, feel free to pick up where we left off
- Be friendly, ask questions!

Thank You!