GNUnet

A network protocol stack for building secure, distributed, and privacy-preserving application

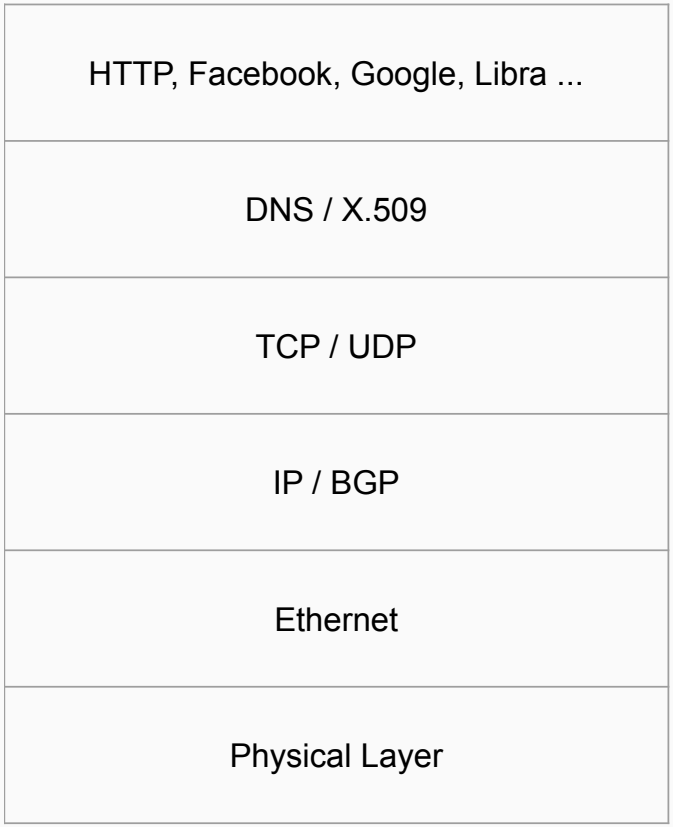
FOSDEM20

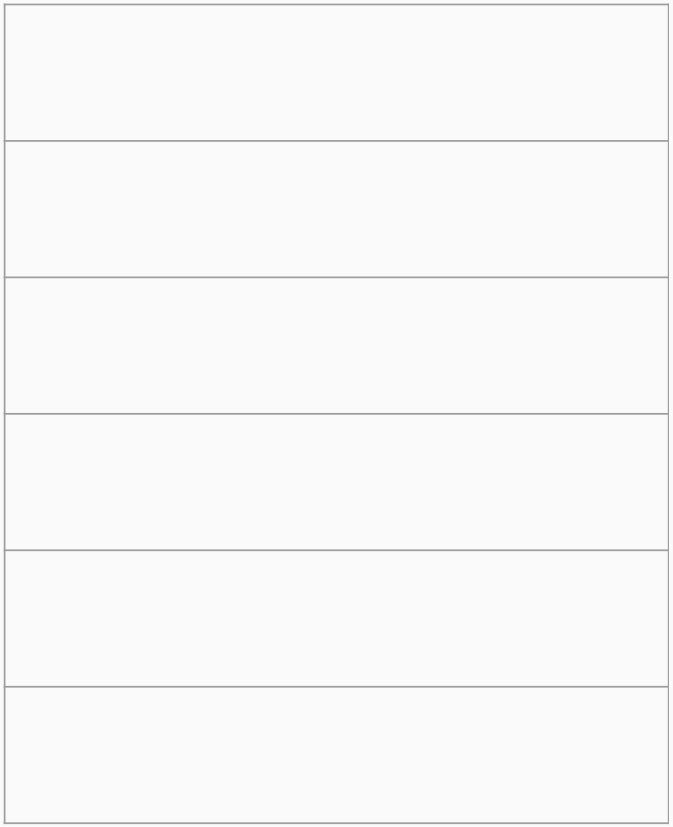
Martin Schanzenbach

2/2/2020

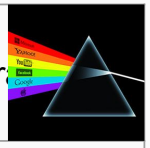
The Internet is under attack

The “Internet”





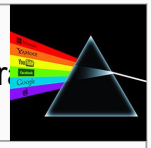
The “Internet”

HTTP, Facebook, Google, Libr 
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer

*Images from eff.org

The “Internet”

HTTP, Facebook, Google, Libra



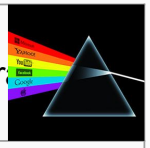
DNS / X.509

TCP / UDP

*Images from eff.org

The “Internet”

HTTP, Facebook, Google, Libr



TCP / UDP

*Images from eff.org

Vision

Full-stack replacement of the Internet infrastructure.

- Metadata protection.
- Encryption.
- Decentralization.


The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
The Wishlist
???

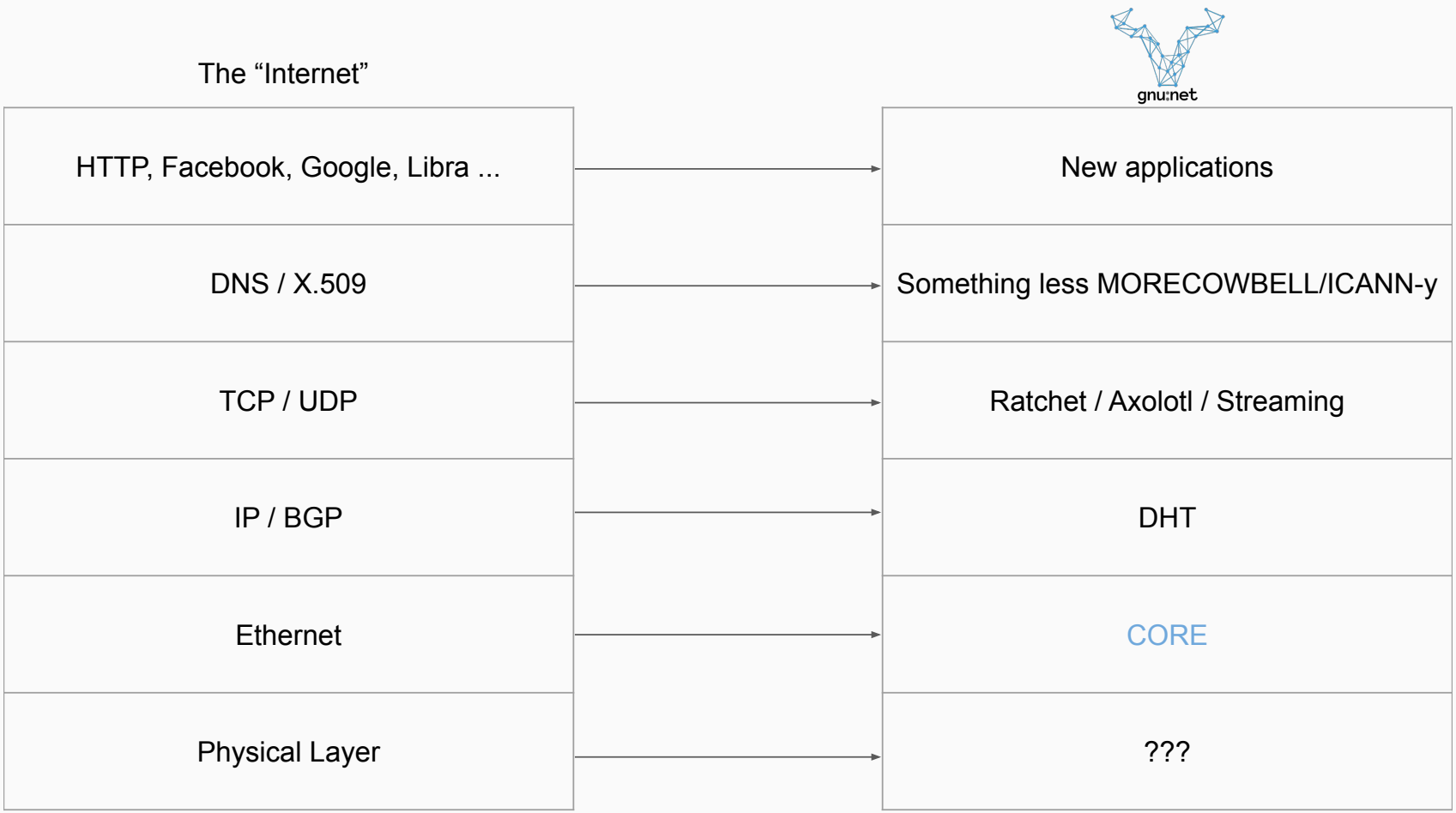

The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
The Wishlist
OTR-like protocol
???

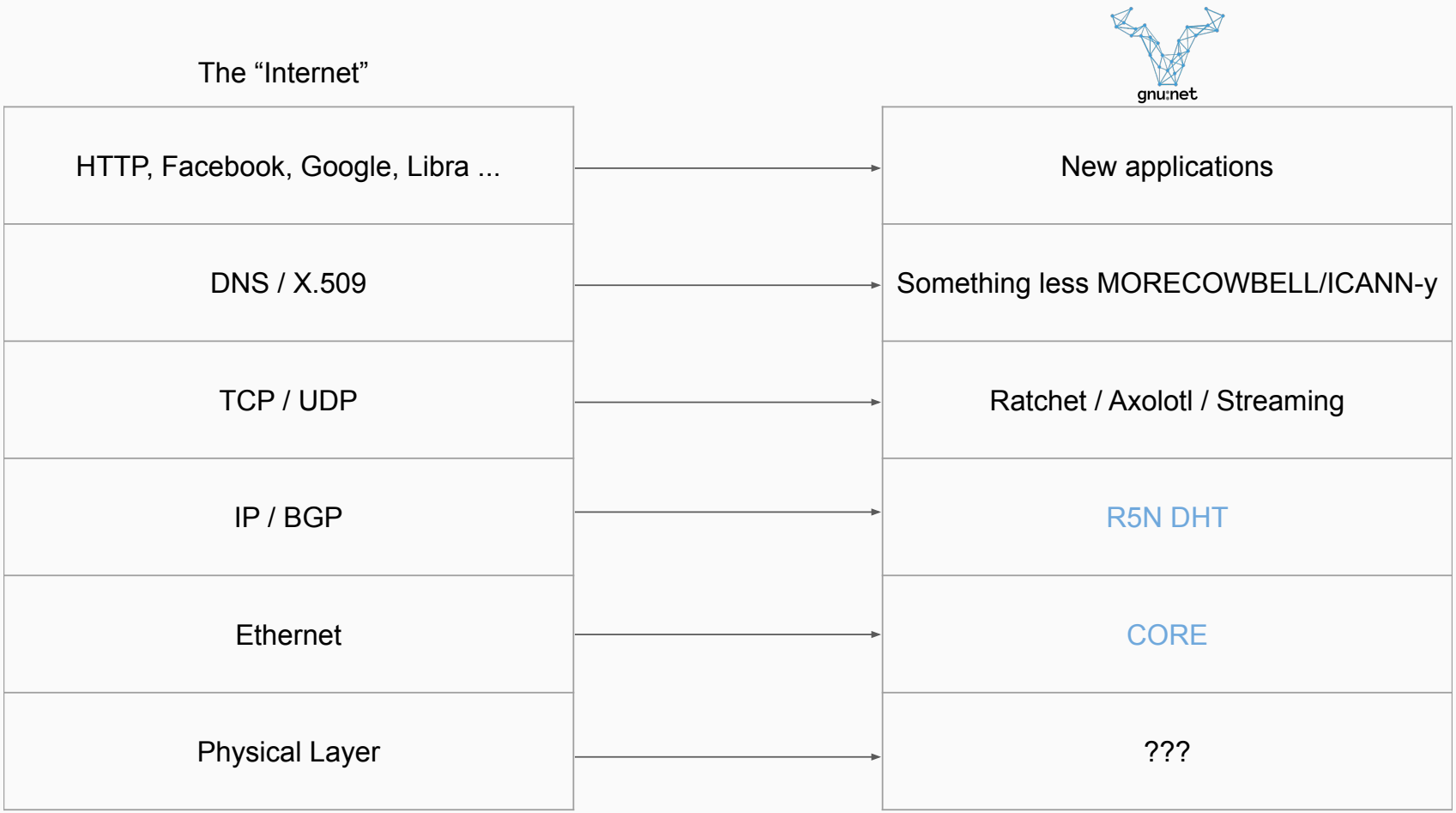

The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
The Wishlist
DHT
OTR-like protocol
???

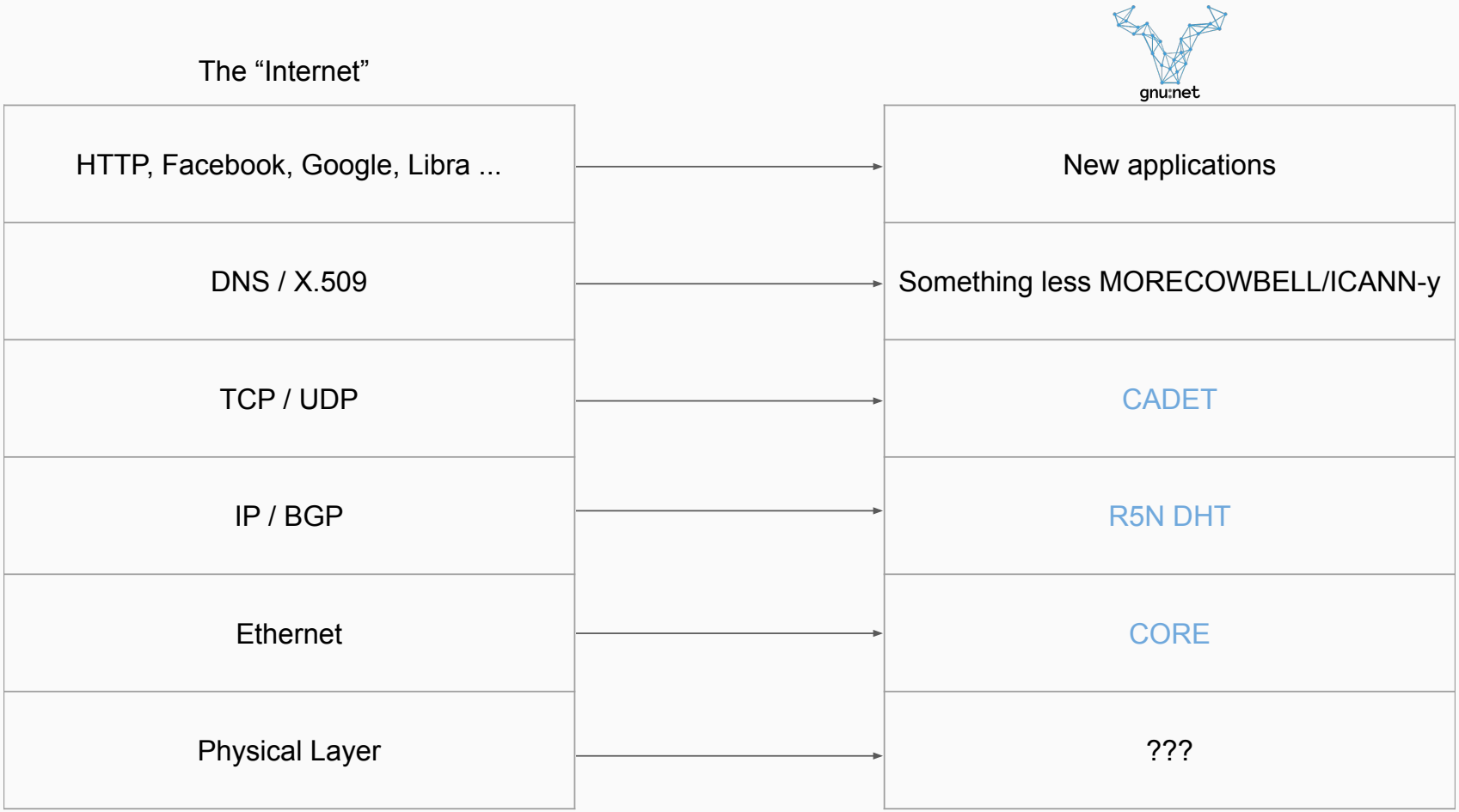

The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
The Wishlist
Ratchet / Axolotl / Streaming
DHT
OTR-like protocol
???

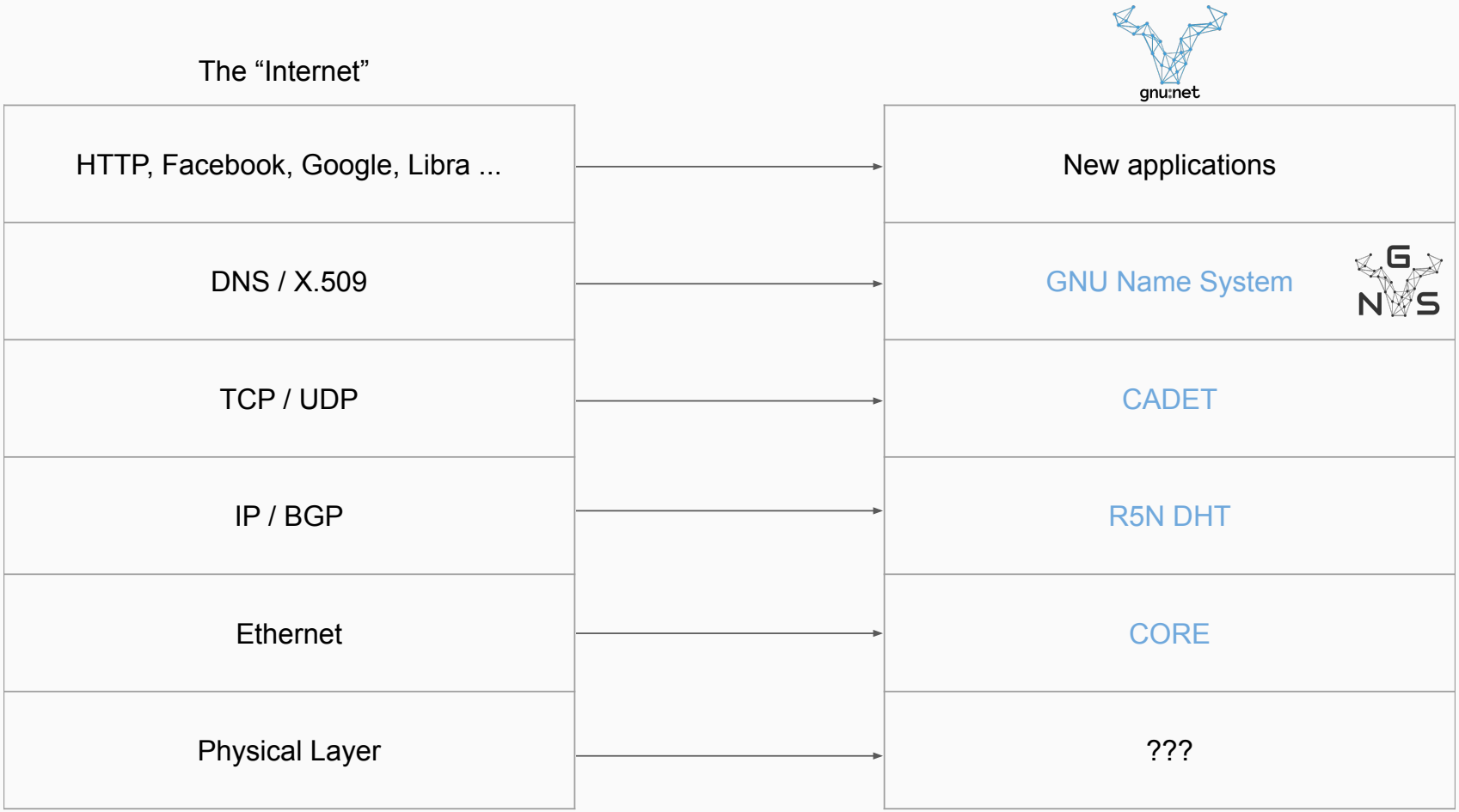

The “Internet”
The Wishlist
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
Something less MORECOWBELL/ICANN-y
Ratchet / Axolotl / Streaming
DHT
OTR-like protocol
???

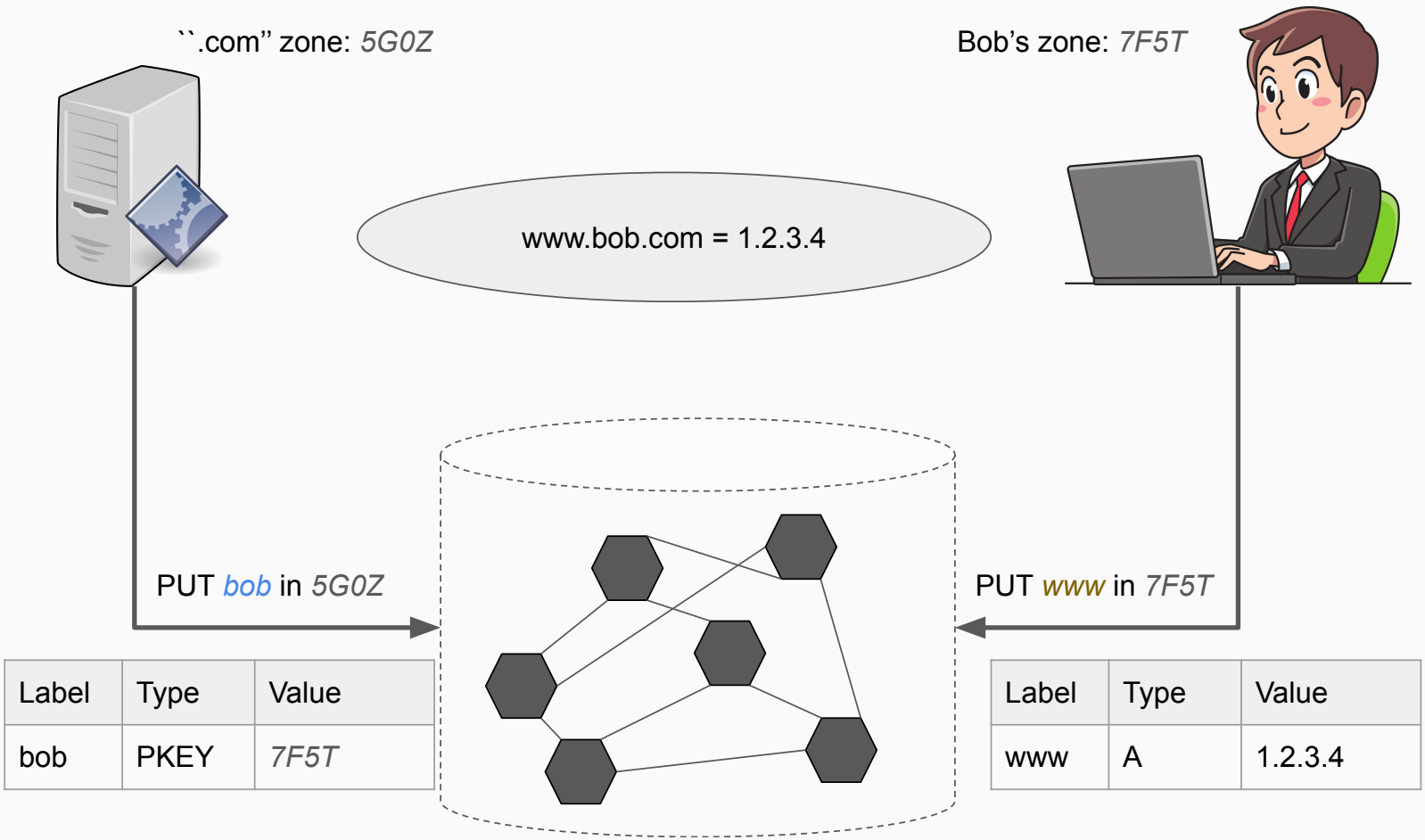

The “Internet”
The Wishlist
HTTP, Facebook, Google, Libra ...
New applications
DNS / X.509
Something less MORECOWBELL/ICANN-y
TCP / UDP
Ratchet / Axolotl / Streaming
IP / BGP
DHT
Ethernet
OTR-like protocol
Physical Layer
???


The “Internet”
gnu:net
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
New applications
Something less MORECOWBELL/ICANN-y
Ratchet / Axolotl / Streaming
DHT
CORE
???


The “Internet”
gnu:net
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
New applications
Something less MORECOWBELL/ICANN-y
Ratchet / Axolotl / Streaming
R5N DHT
CORE
???

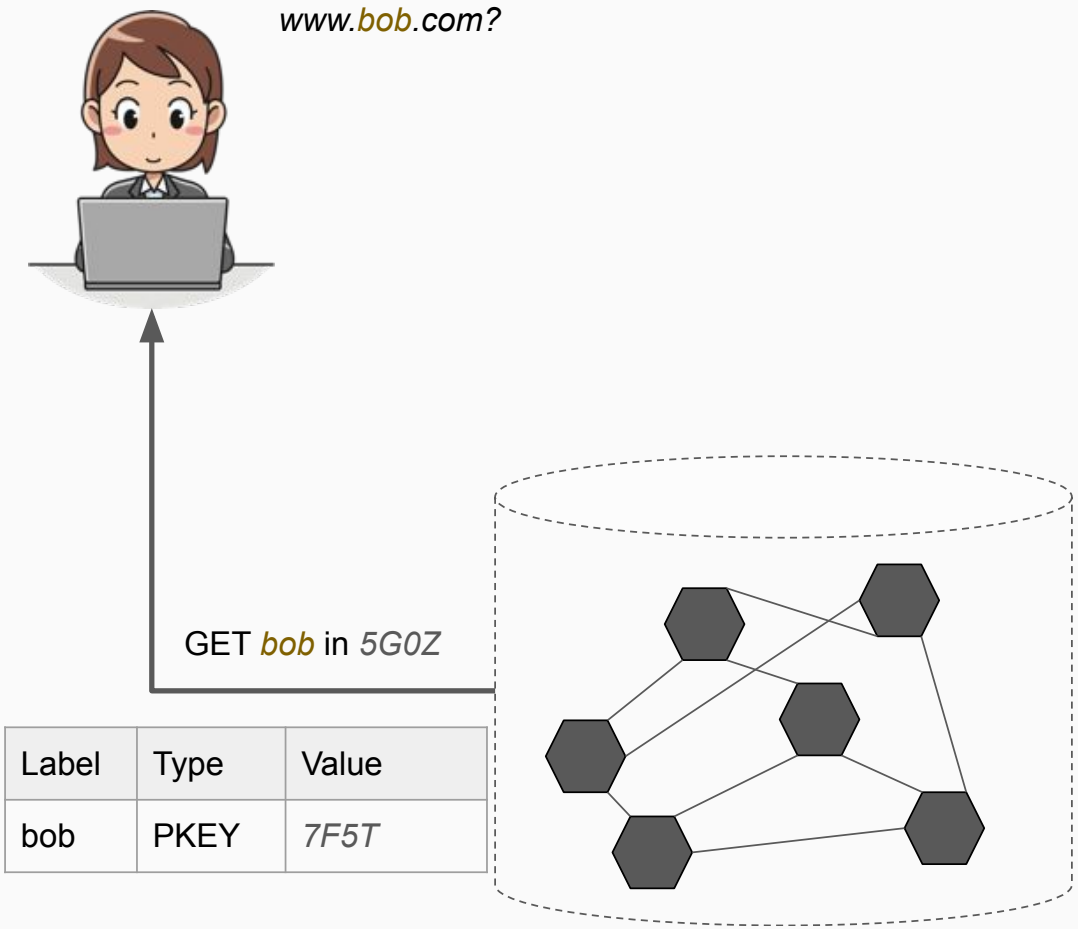

The “Internet”
gnu:net
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
New applications
Something less MORECOWBELL/ICANN-y
CADET
R5N DHT
CORE
???

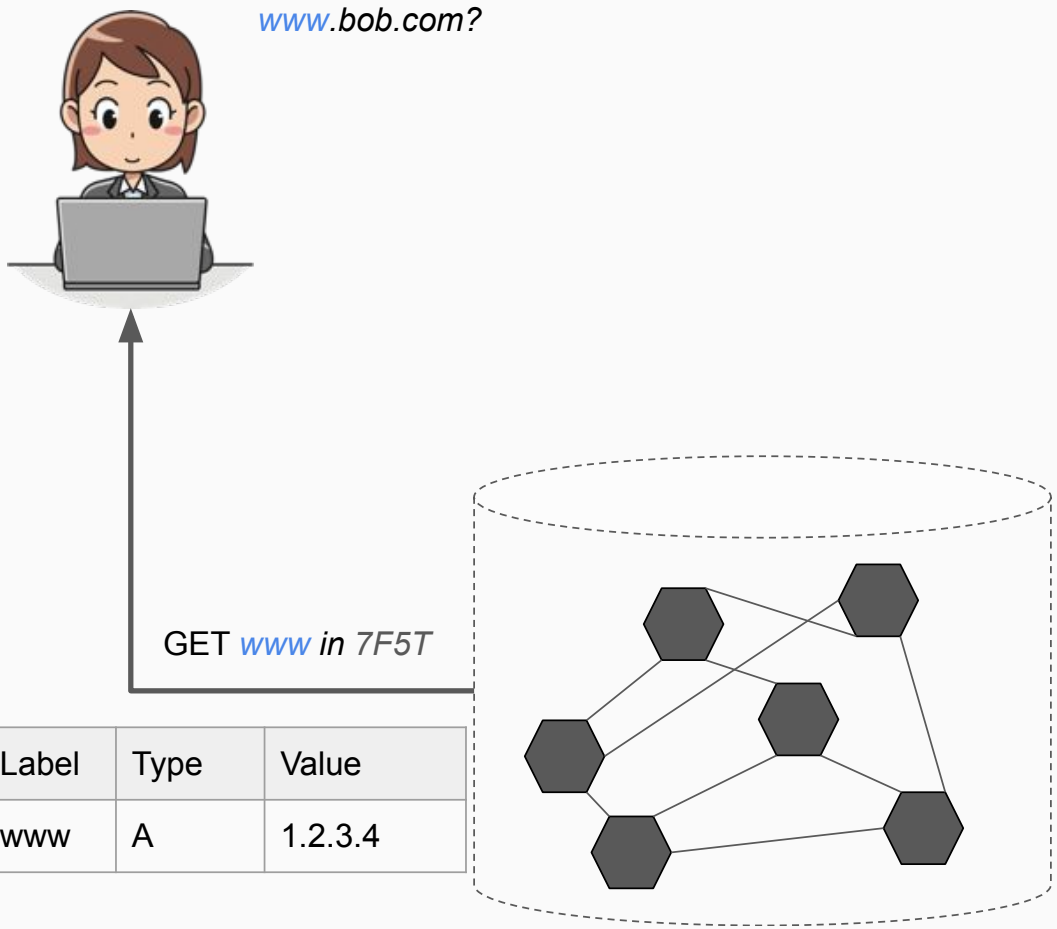

The “Internet”
gnu:net
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
New applications
GNU Name System
CADET
R5N DHT
CORE
???



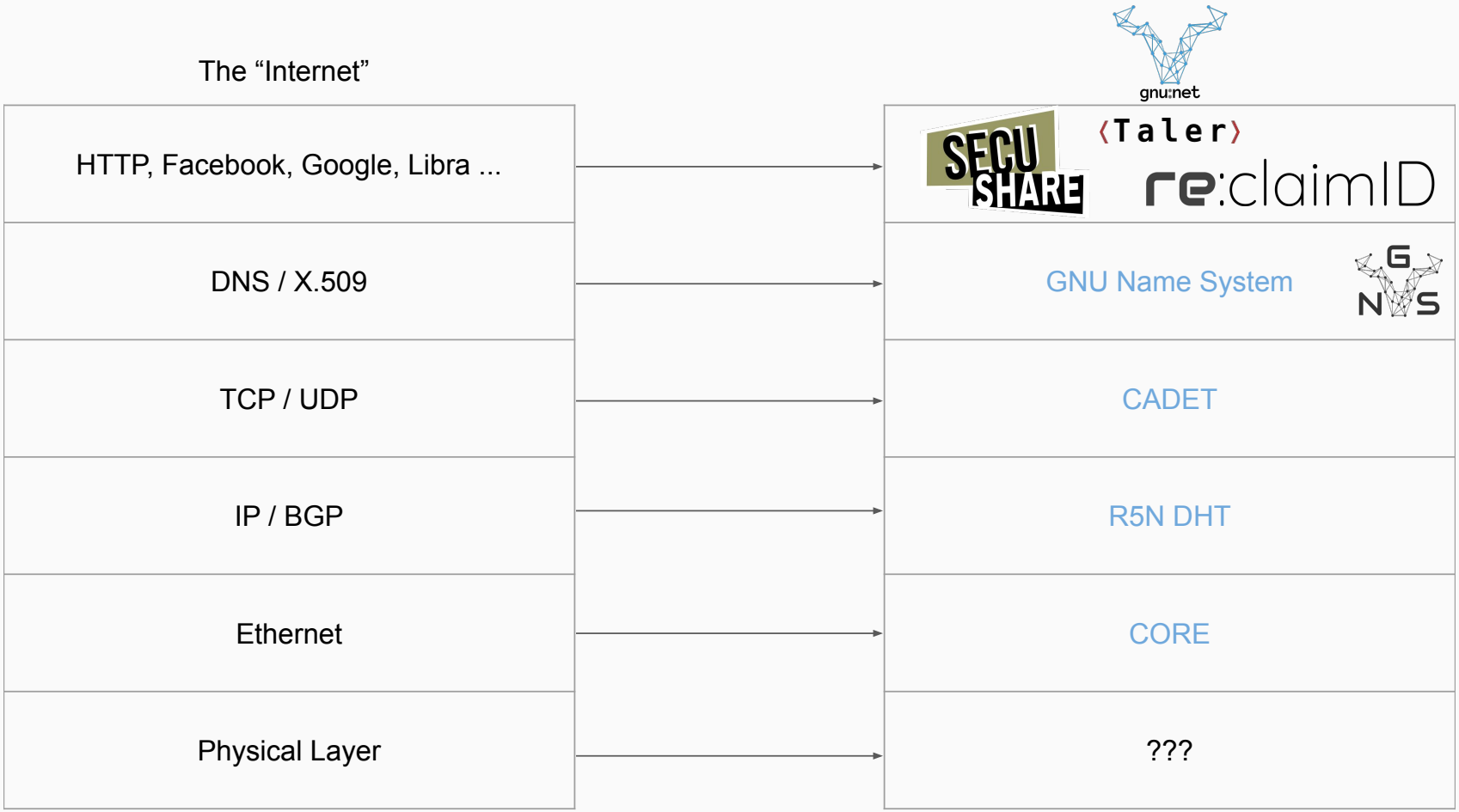
Label	Type	Value
bob	PKEY	*7F5T*

Label	Type	Value
www	A	1.2.3.4

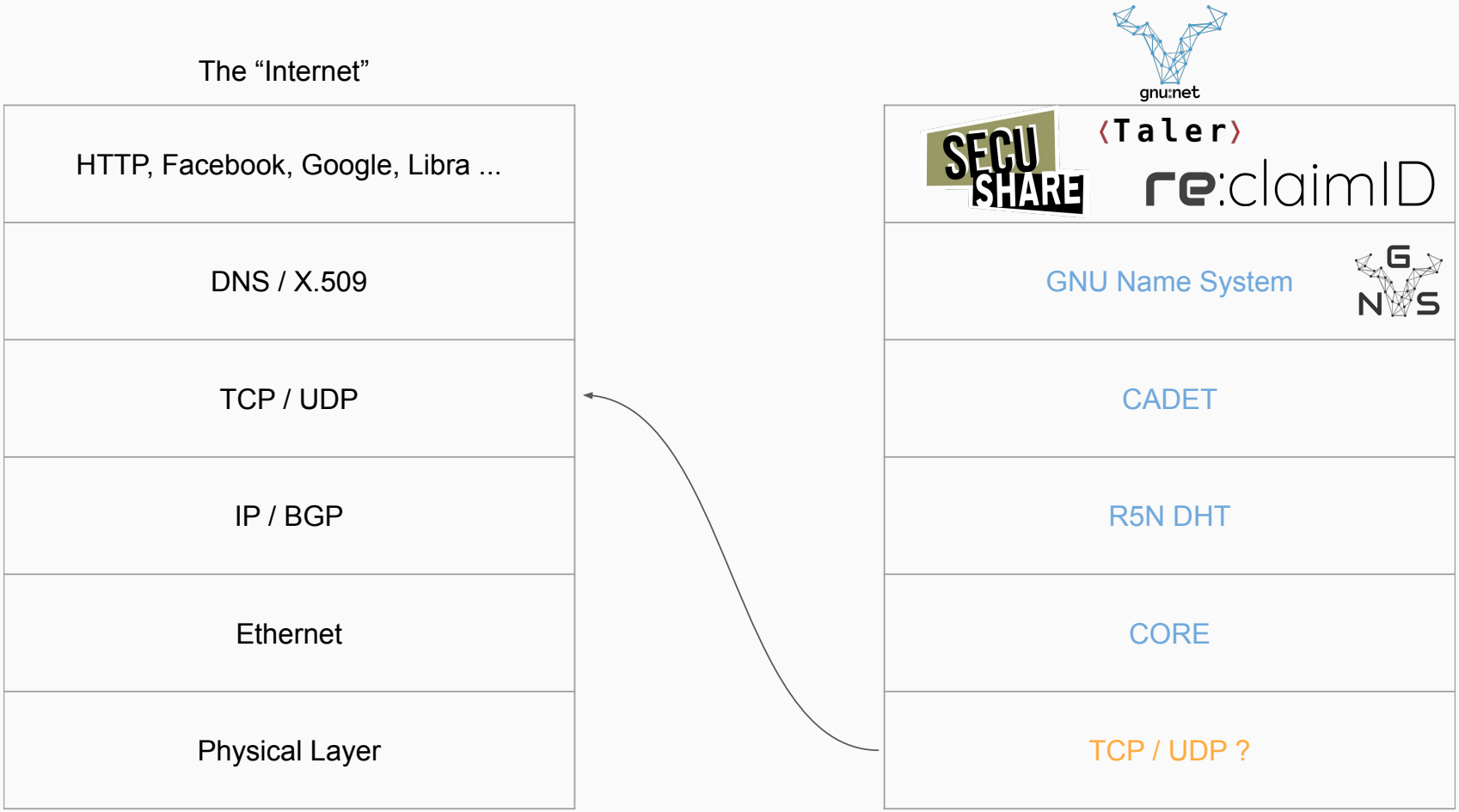

www.bob.com?
GET bob in 5G0Z
Label
Type
Value
bob
PKEY
7F5T

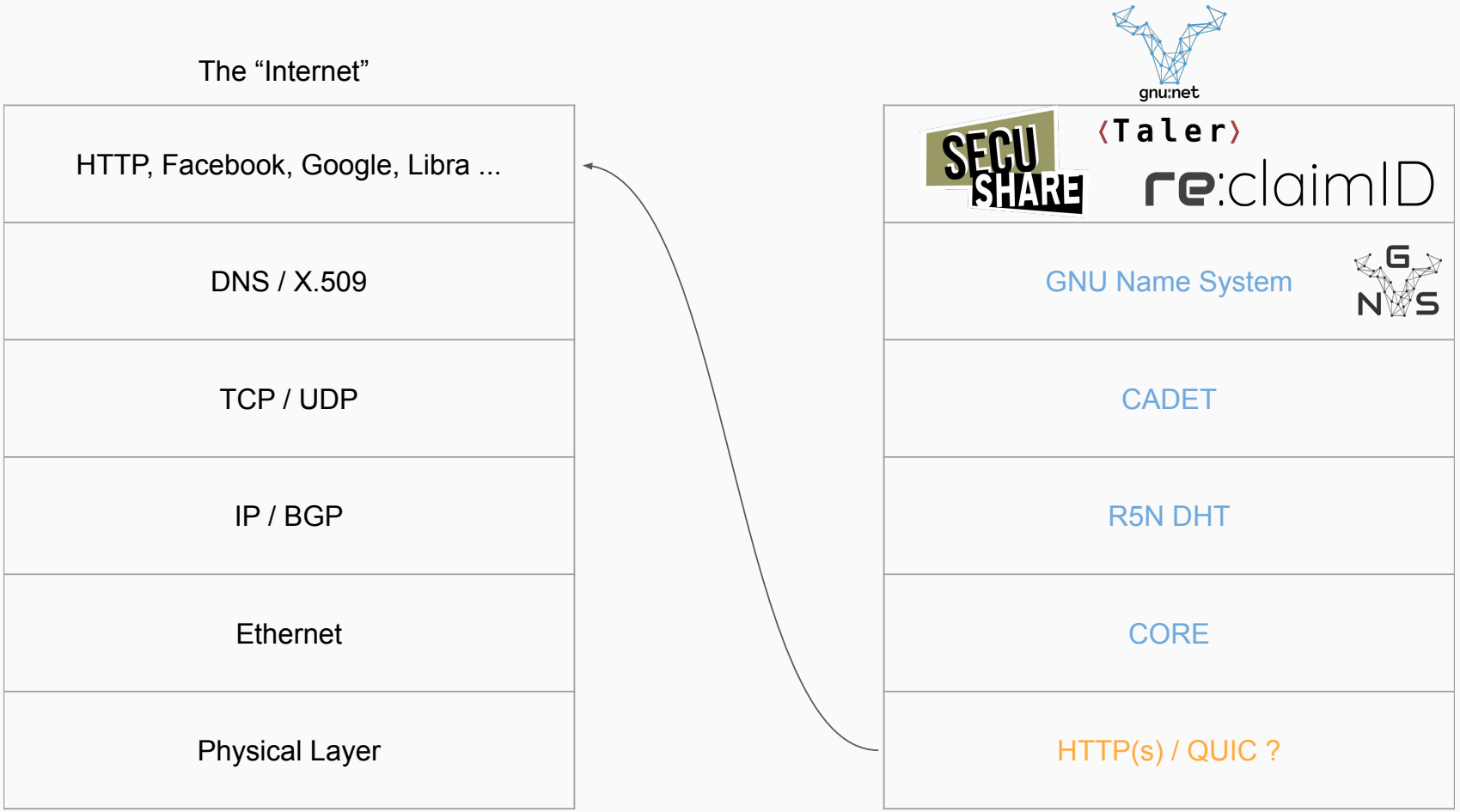


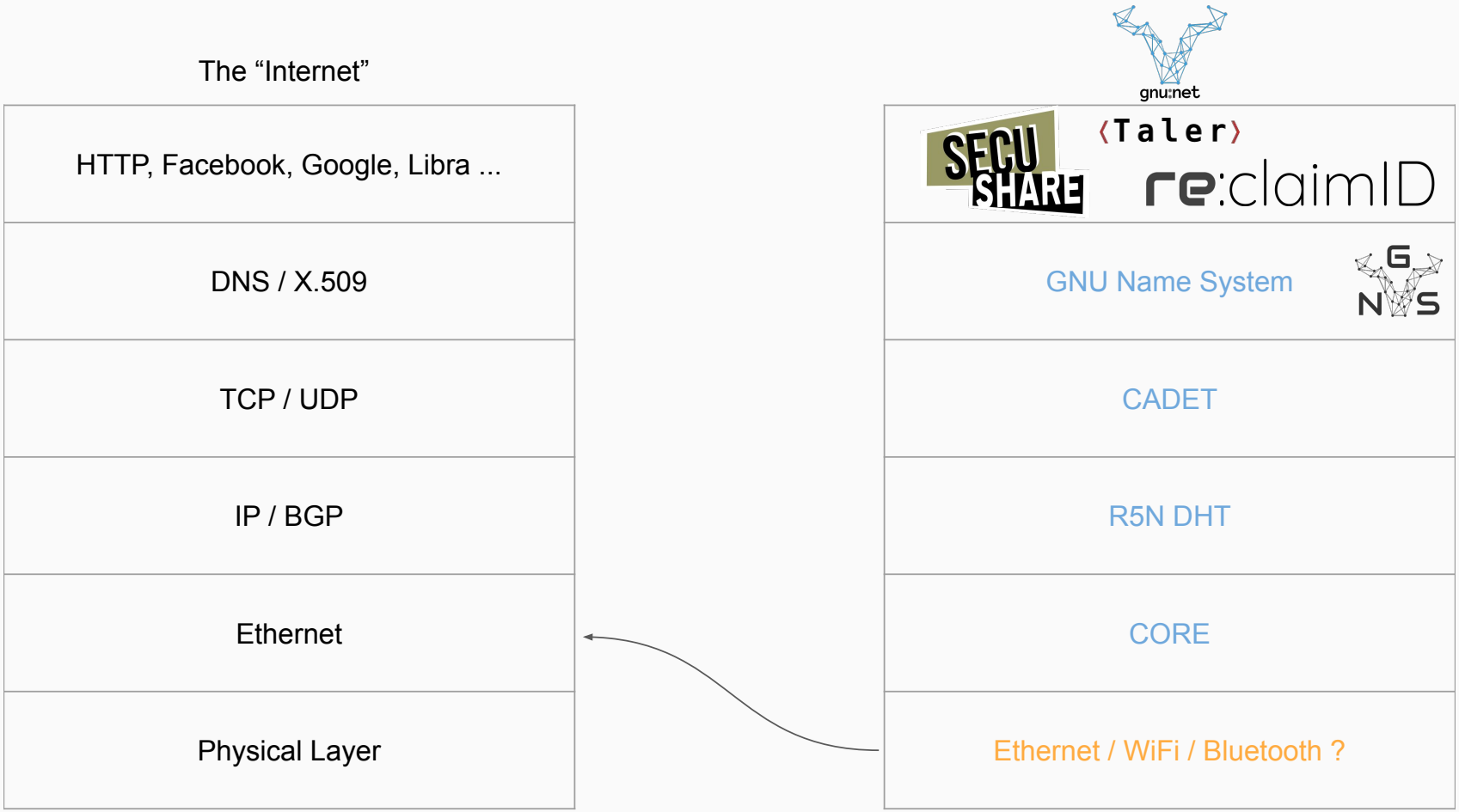
Label	Type	Value
www	A	1.2.3.4


The “Internet”
gnu:net
HTTP, Facebook, Google, Libra ...
SECU SHARE
⟨Taler⟩
re:claimID
DNS / X.509
GNU Name System
G
N S
TCP / UDP
CADET
IP / BGP
R5N DHT
Ethernet
CORE
Physical Layer
???

re:claimID = +


The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
gnu:net
SECU SHARE
⟨Taler⟩
re:claimID
GNU Name System
G N S
CADET
R5N DHT
CORE
TCP / UDP ?

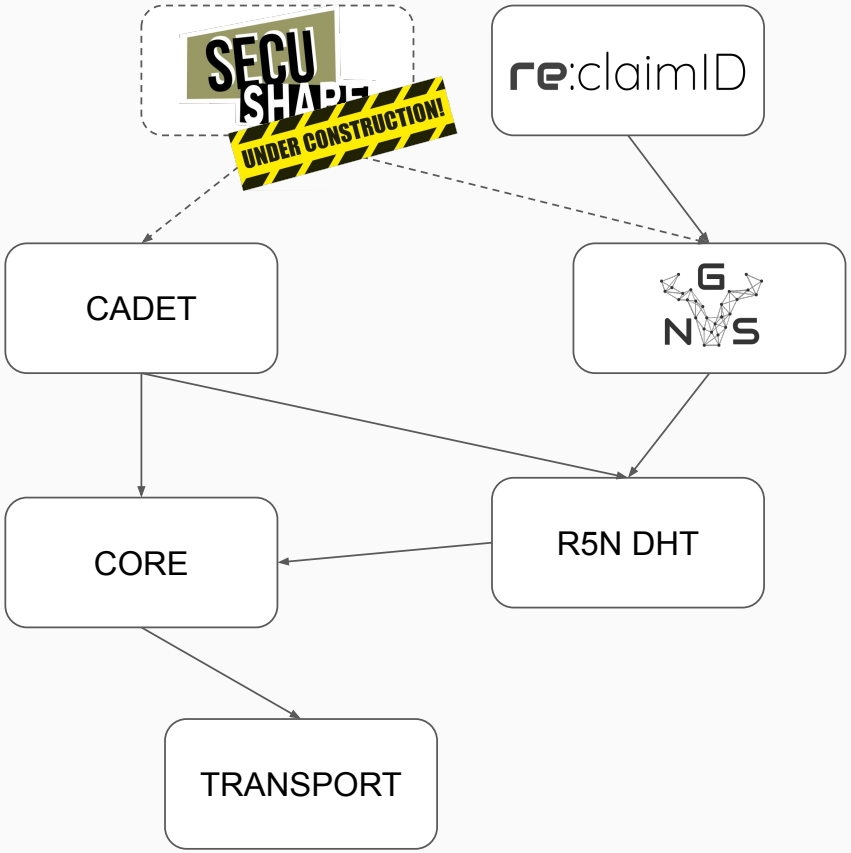

The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
gnu:net
SECU SHARE
⟨Taler⟩
re:claimID
GNU Name System
G N S
CADET
R5N DHT
CORE
HTTP(s) / QUIC ?


The “Internet”
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer
gnu:net
SECU SHARE
⟨Taler⟩
re:claimID
GNU Name System
G N S
CADET
R5N DHT
CORE
Ethernet / WiFi / Bluetooth ?

The “Internet”

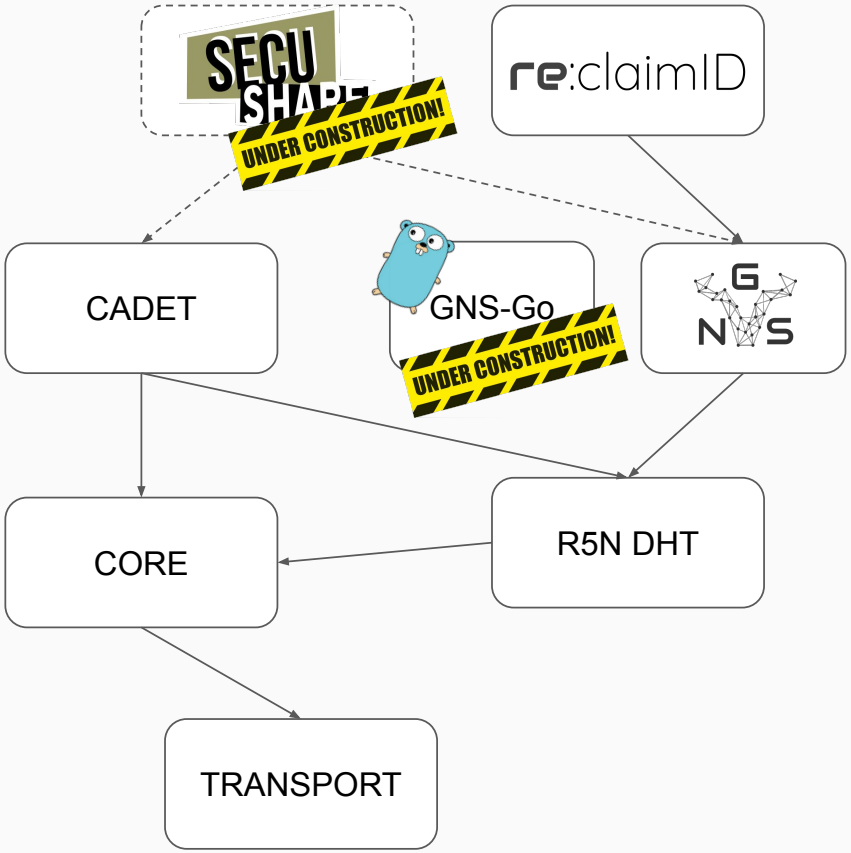
HTTP, Facebook, Google, Libra ...
DNS / X.509
TCP / UDP
IP / BGP
Ethernet
Physical Layer

SECU SHARE ⟨Taler⟩ re:claimID				
GNU Name System				
CADET				
R5N DHT				
CORE				
TRANSPORT				
TCP/UDP	HTTP(s)	WiFi	Bluetooth	...



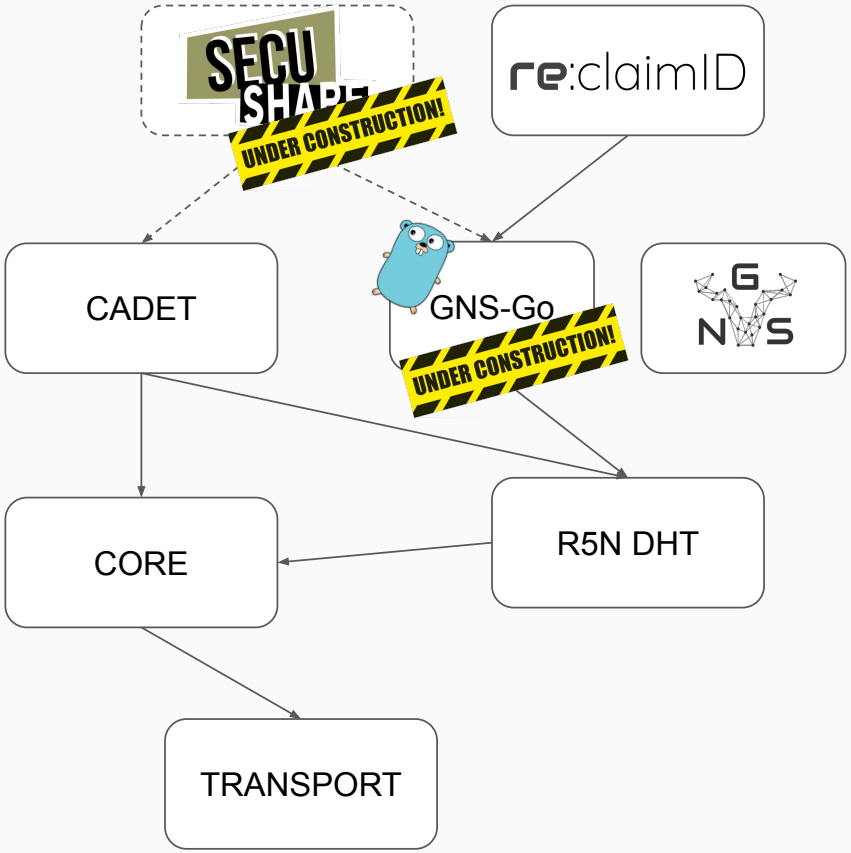
= Service / Process

= Dependency / Socket



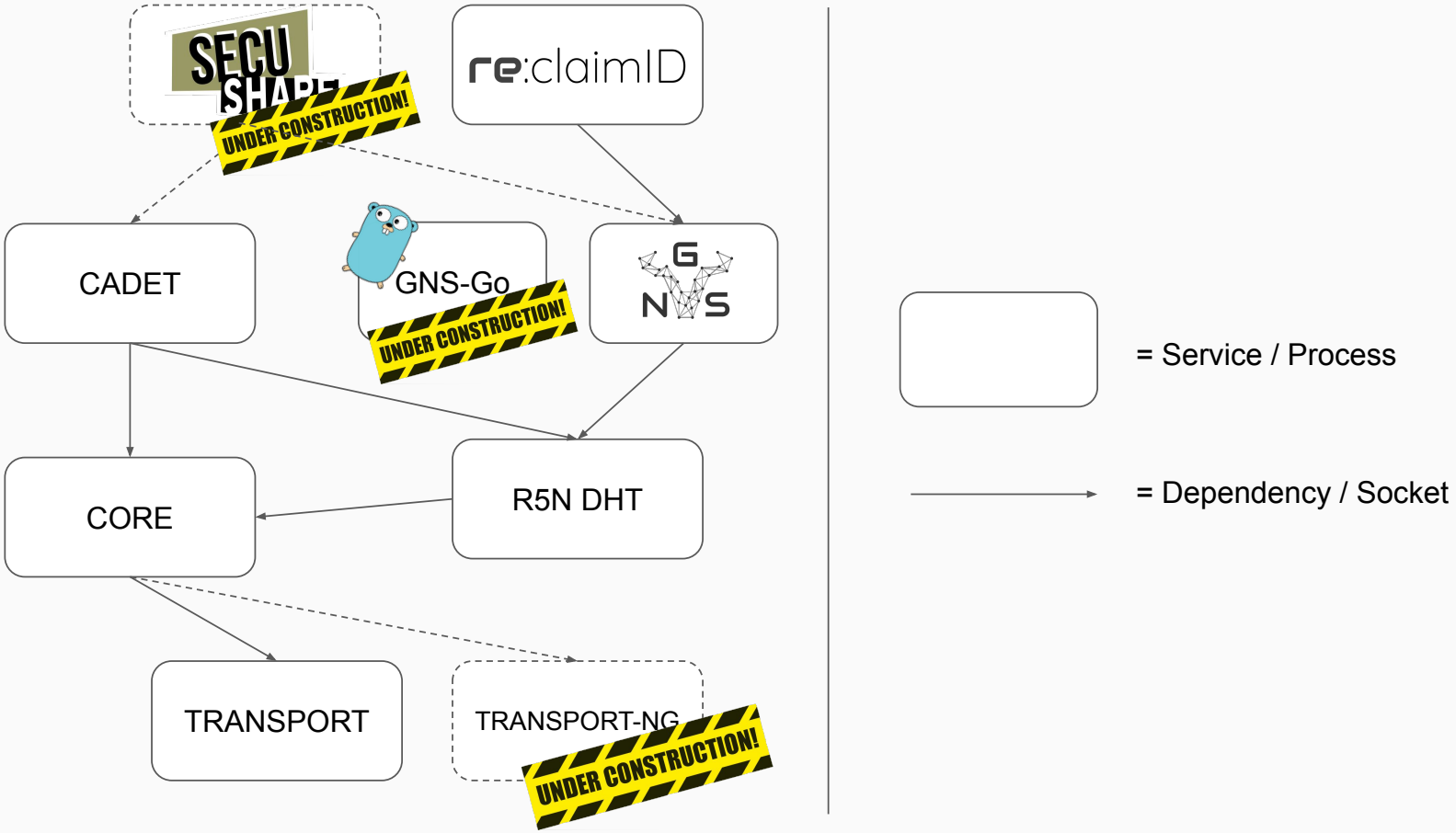
= Service / Process

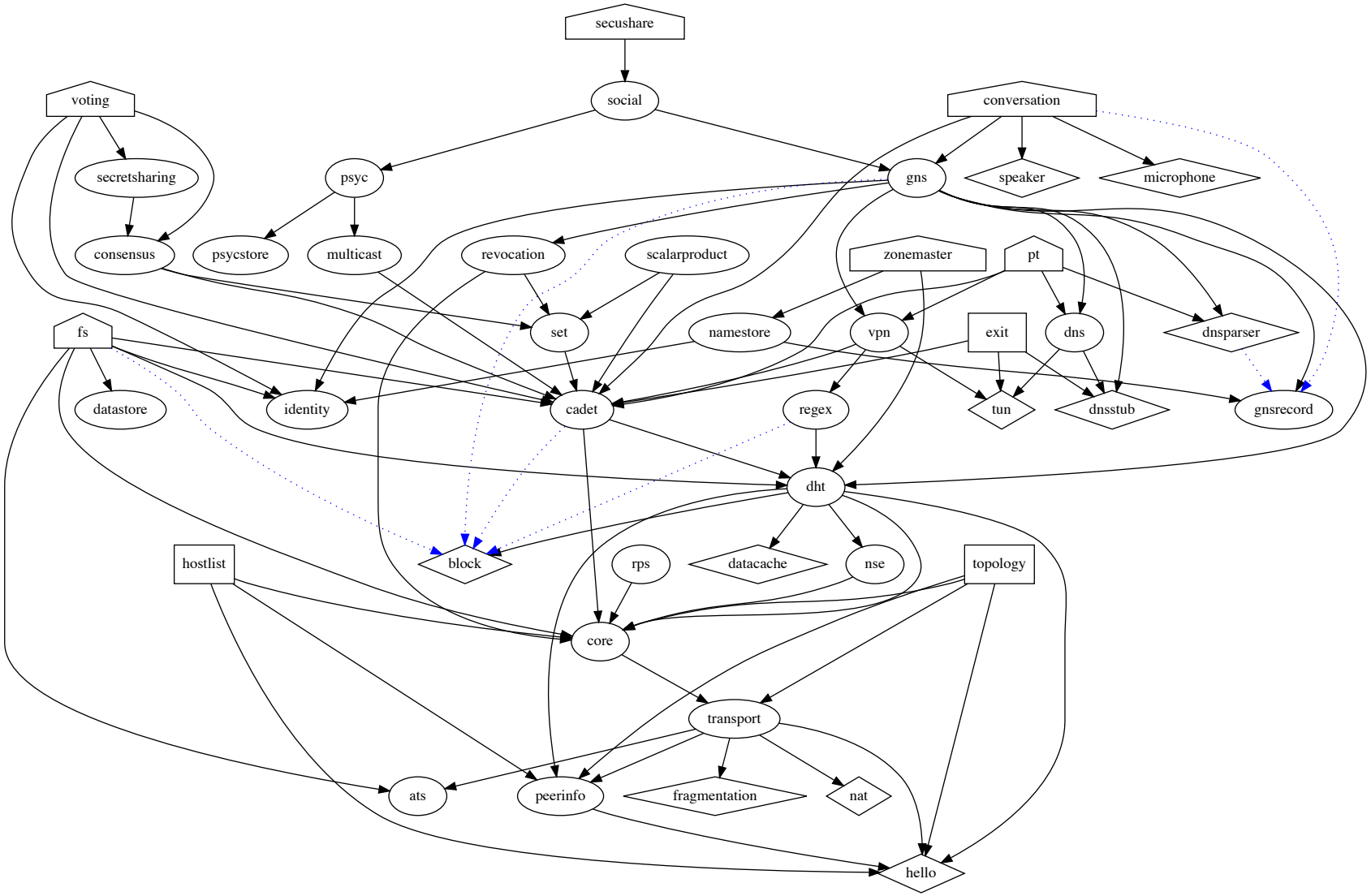
= Dependency / Socket



= Service / Process

= Dependency / Socket


SECU SHARE
UNDER CONSTRUCTION!
re:claimID
CADET
GNS-Go
UNDER CONSTRUCTION!
G N S
CORE
R5N DHT
TRANSPORT
TRANSPORT-NG
UNDER CONSTRUCTION!
= Service / Process
= Dependency / Socket


secushare
social
voting
conversation
secretsharing
psyc
gns
speaker
microphone
consensus
psycstore
multicast
revocation
scalarproduct
zonemaster
pt
fs
set
namestore
vpn
exit
dns
dnsparser
datastore
identity
cadet
regex
tun
dnsstub
gnsrecord
dht
hostlist
block
rps
datacache
nse
topology
core
transport
ats
peerinfo
fragmentation
nat
hello

Quo Vadis?

2020/2021:

- Make progress with transport redesign/rewrite.
- GNS standardization, documentation.
- GNS alternative implementation (Go).
- Next major releases: 0.13/0.14

Beyond:

- SecuShare
- Additional transports: WiFi/Mesh, Bluetooth, QUIC ...
- GNS `.org` replacement authority.

https://gnunet.org

schanzen@gnunet.org
3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A

References

1. Bart Polot and Christian Grothoff. **CADET: Confidential Ad-hoc Decentralized End-to-End Transport**. *13th IEEE IFIP Annual Mediterranean Ad Hoc Networking Workshop*, 2014
2. Nathan S. Evans and Christian Grothoff. **R5N: Randomized Recursive Routing for Restricted-Route Networks**. *5th International Conference on Network and System Security*, 2011.
3. Matthias Wachs, Martin Schanzenbach and Christian Grothoff. **A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System**. *13th International Conference on Cryptology and Network Security*, 2014.
4. Christian Grothoff. **The GNUnet System**. *Thèse d'habilitation à diriger des recherches*. 2017.
5. Martin Schanzenbach, Georg Bramm, Julian Schütte. **reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption**. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, 2018