ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Collective Authorities

Transparency and Decentralized Trust at Scale

Philipp Jovanovic

@Daeinar

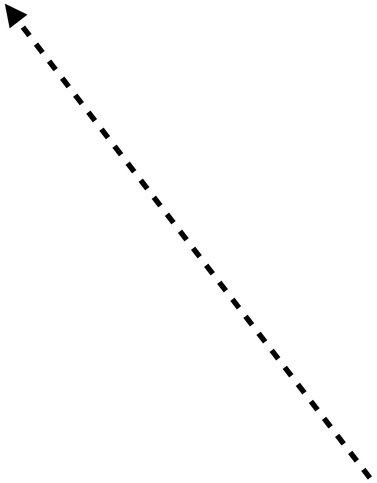
Deep Dependence on Internet Authorities

Time Service

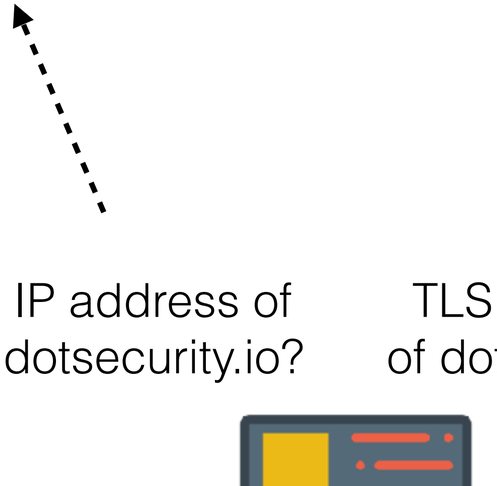
Naming Authority

Certificate Provider

Software Update Center

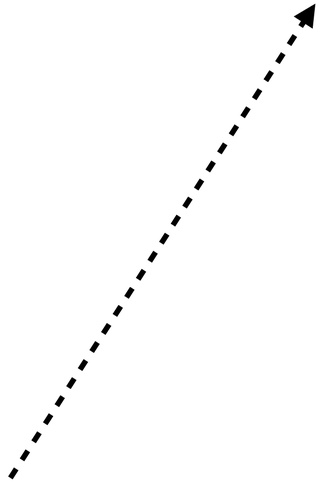


Current time?

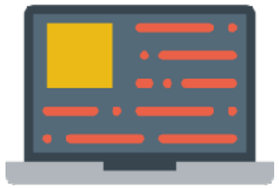


IP address of dotsecurity.io?

TLS certificate of dotsecurity.io?



New updates?



Client

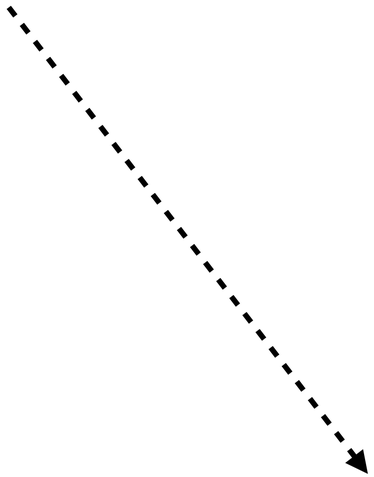
Authorities Make and Sign Statements

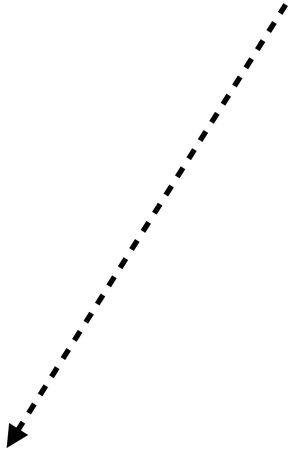
Time Service

Naming Authority

Certificate Provider

Software Update Center



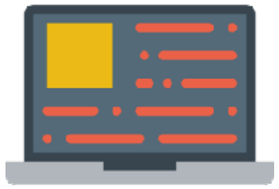


It is **17:05**.

IP address is **104.24.103.23**.

TLS certificate is **xyz**.

New security update **1.0.1.2** available.



Client

Authority Compromise

Time Service

Naming Authority

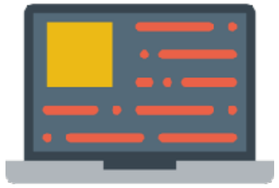
Certificate Provider

Software Update Center

It is **10:00**.

IP address is **104.24.103.23**.

TLS certificate is **xyz**.



Client

New security update **1.0.1.2** available.

Authority Compromise

Time Service

Naming Authority

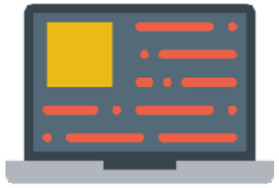
Certificate Provider

Software Update Center

It is **10:00**.

IP address is **95.123.101.20**.

TLS certificate is **xyz**.



Client

New security update **1.0.1.2** available.

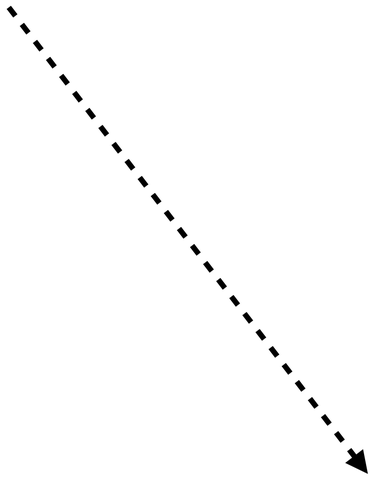
Authority Compromise

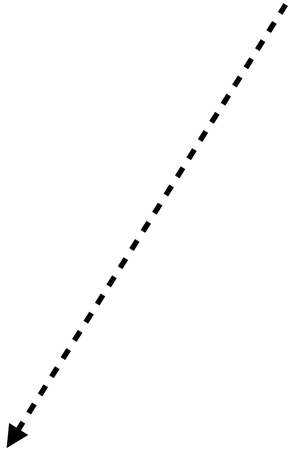
Time Service

Naming Authority

Certificate Provider

Software Update Center

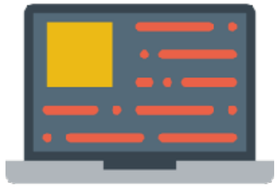




IP address is **95.123.101.20**.

TLS certificate is **zyx**.

It is **10:00**.



Client

New security update **1.0.1.2** available.

Authority Compromise

Time Service

Naming Authority

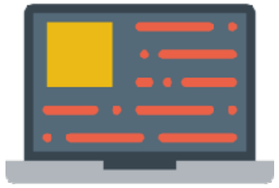
Certificate Provider

Software Update Center

It is **10:00**.

IP address is **95.123.101.20**.

TLS certificate is **zyx**.



Client

New security update **1.0.1.1** available.

Technical Threats

Adobe Revoking Code Signing Certificate Used To Sign Malware

Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs [updated]

Chrome to immediately stop recognizing EV status and gradually nullify all certs.

DAN GOODIN - 3/24/2017, 4:22 PM

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - 2/19/2015, 5:36 PM

Second Dell backdoor root cert found

Blackhats, head straight to the airport lounge.

25 Nov 2015 at 05:00, Darren Pauli

Trustwave Admits It Issued A Certificate To Allow Company To Run Man-In-The-Middle Attacks

DigiNotar scandal worsens: 500+ rogue certificates issued, five CAs breached

Man hacked random-number generator to rig lotteries, investigators say

New evidence shows lottery machines were rigged to produce predictable jackpot numbers on specific days of the year netting millions in winnings

New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

DAN GOODIN - 10/22/2015, 12:07 AM

Legal Threats

“Hey Lavabit, give us your crypto keys. Ah and you can’t tell anybody about it.”

vs.

“Grml, here. To save space they are printed in 4pt font. You’re welcome.“

Lavabit shutdown to avoid being complicit in crimes against customers.

Legal Threats

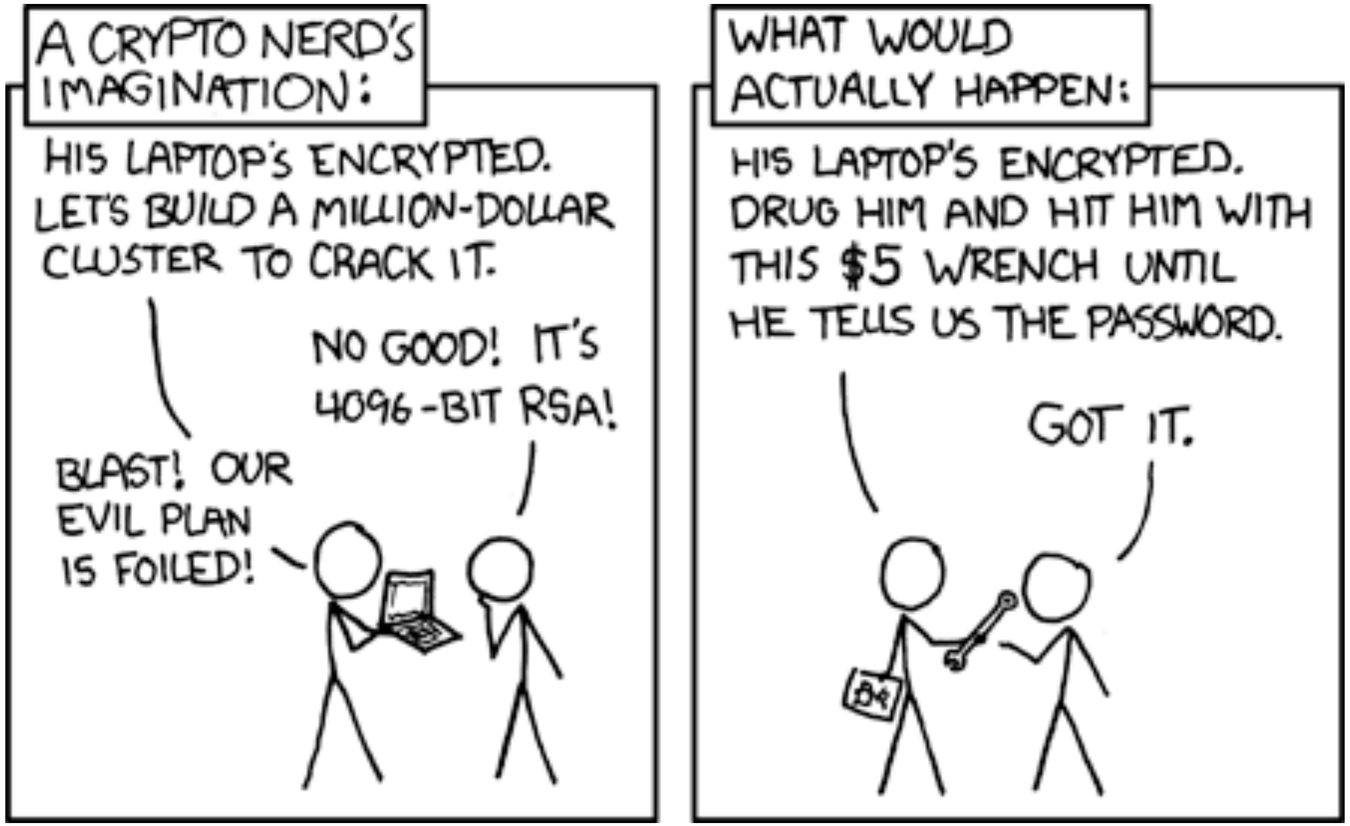
“Hey Apple, create and sign a backdoored iOS.”

vs.

“Hahaha. No.”

Public debate this time, but what about the next round?

Fact:
No Individual Entity is Immune to Compromise or Coercion



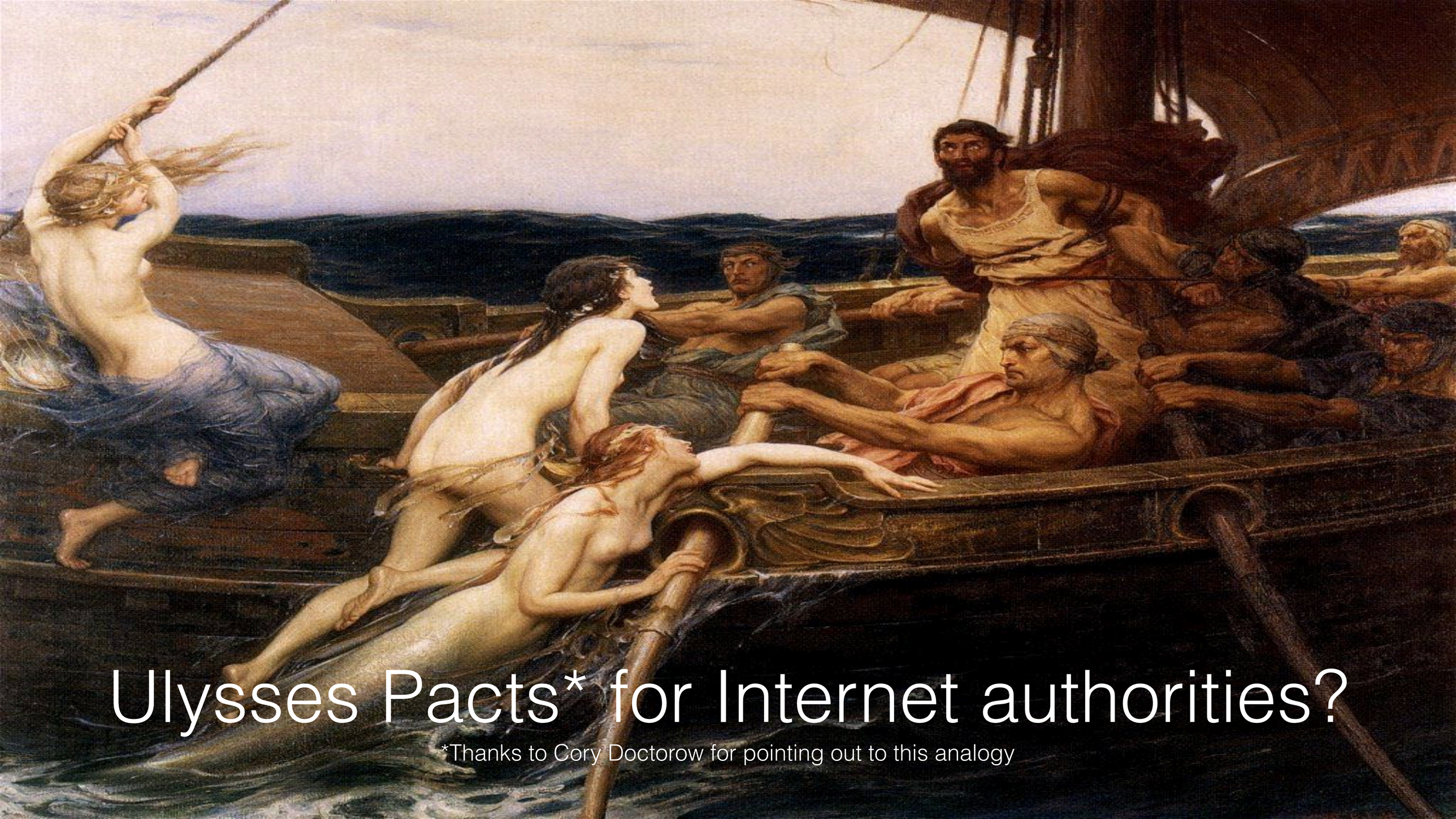
Legal Self-Defense

The FBI has not been here

[watch very closely for removal of this sign]

A warrant canary

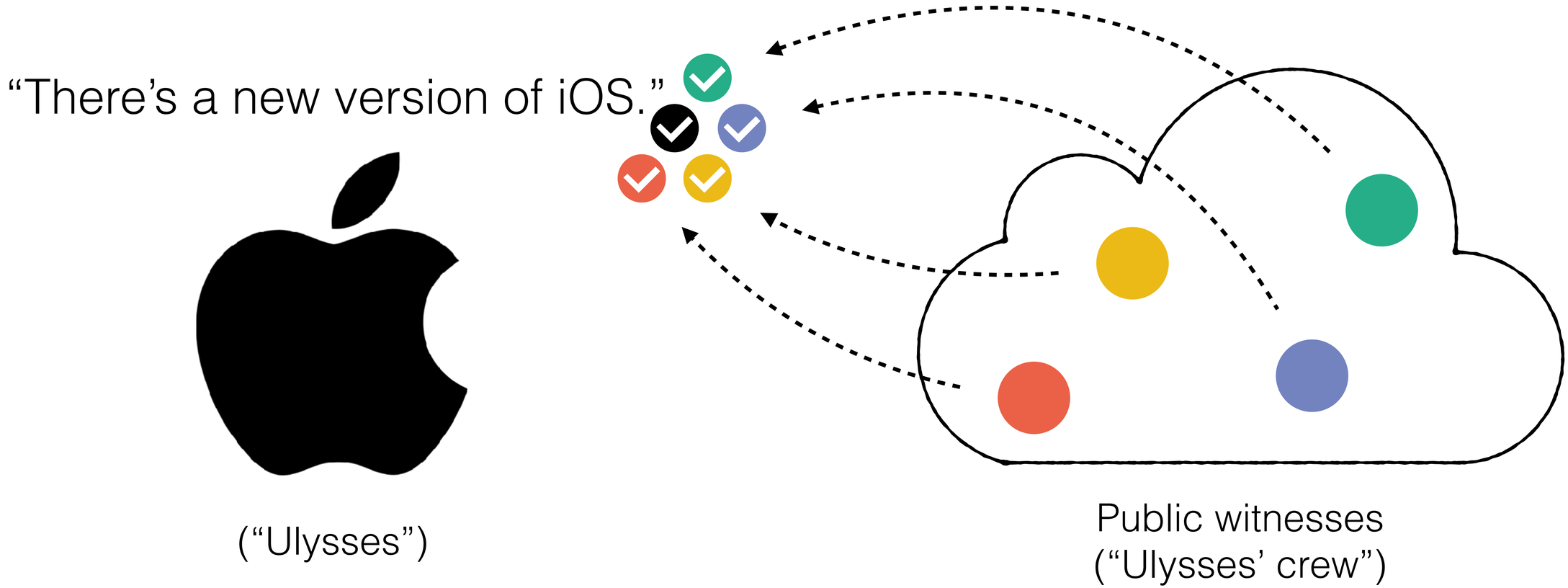
An actual canary



Ulysses Pacts* for Internet authorities?

*Thanks to Cory Doctorow for pointing out to this analogy

Towards Ulysses Pacts for Internet Authorities

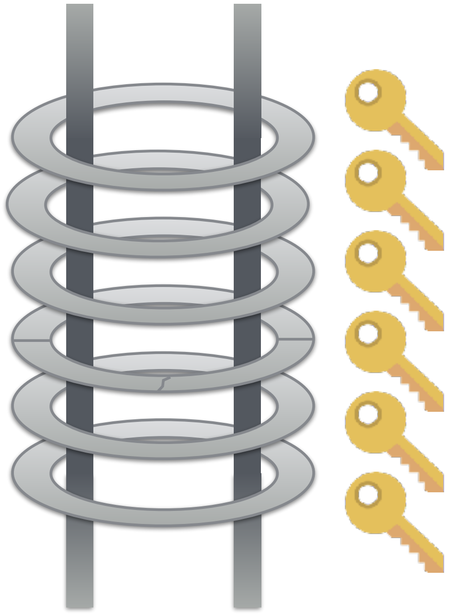


Clients only accept an update if Apple **and** enough public witnesses signed it off.

Towards Ulysses Pacts for Internet Authorities

Weakest link
T = 1

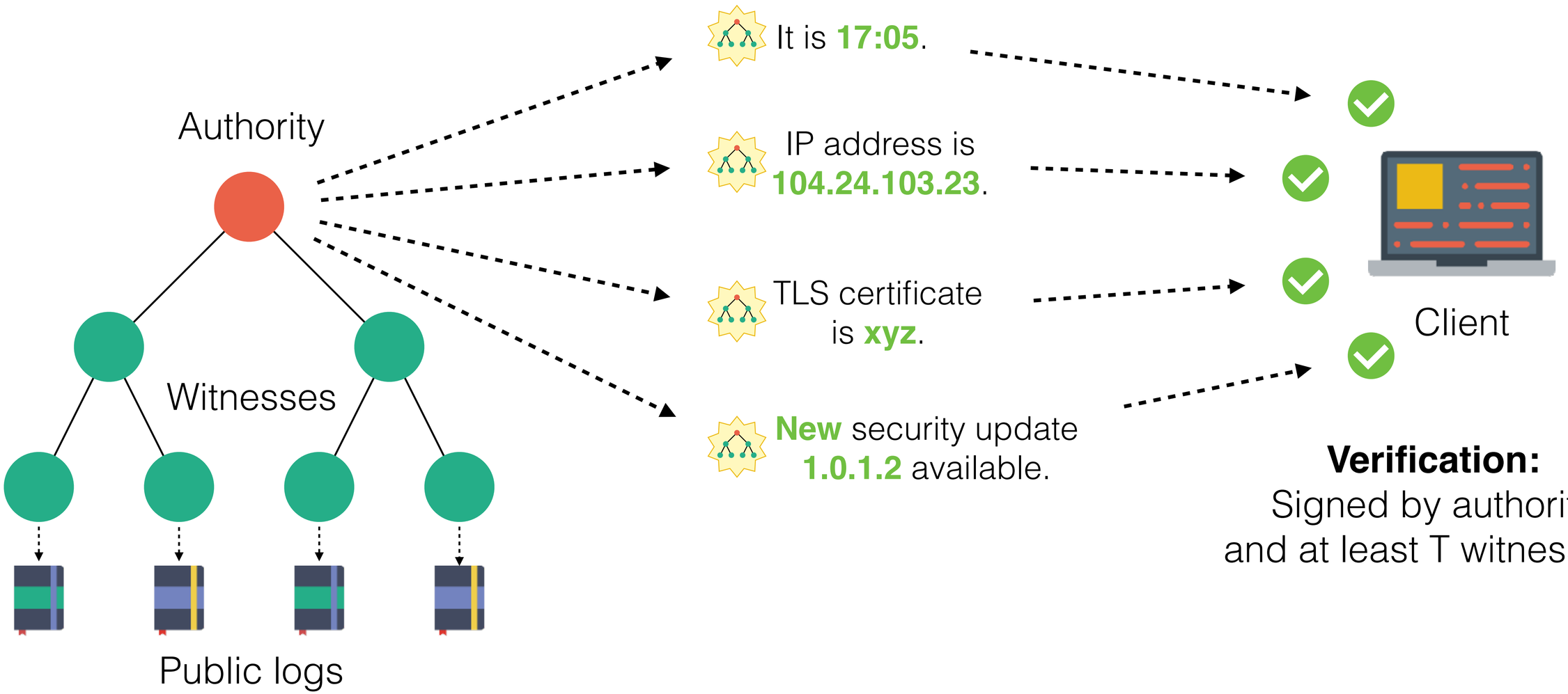
Stronger link
T = 2 … 10



Collective authorities
T = 100++

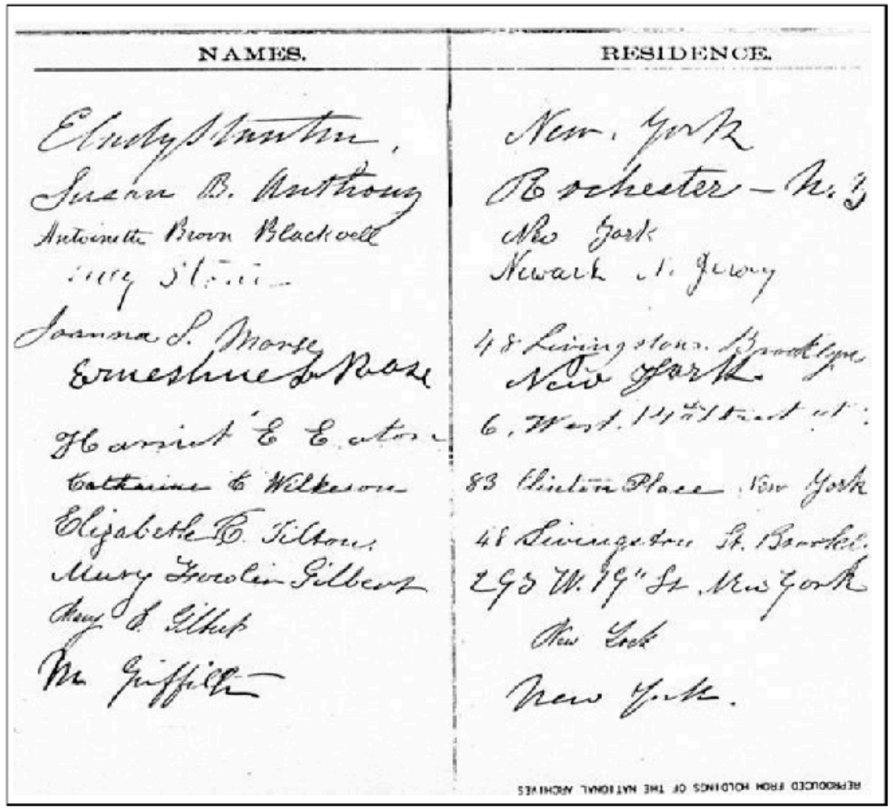
Trust splitting has to scale and increase security, diversity, and independence.

Decentralized Witness Cosigning



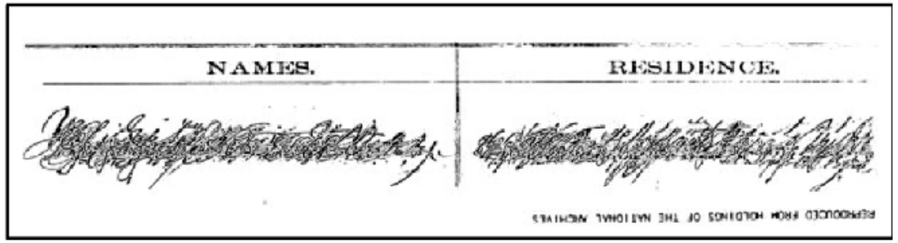
Regular Versus Collective Signing

Excerpt of a public petition from 1866



Regular signatures

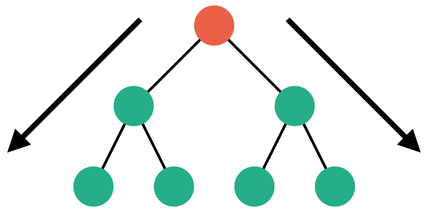
Signatures in superposition



 Collective signature

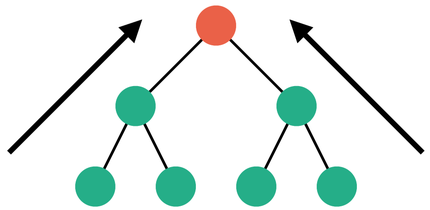
Collective Signing (CoSi)

1. Announcement



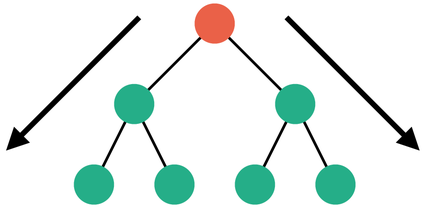
Send statement S
now or later

2. Commitment



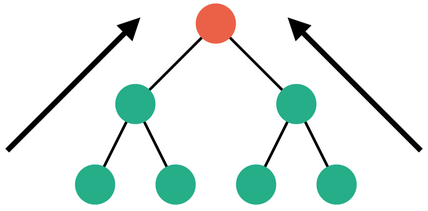
Aggregate commits
$V = \sum_i(v_i G)$

3. Challenge



Send challenge
c = H(V, S)

4. Response



Aggregate responses
r = $\sum_i(v_i - cx_i)$

Collective (Schnorr) signature: (**c**,**r**)

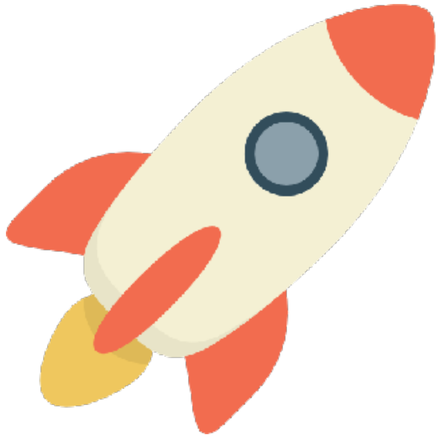
CoSi Features

Security

- Strongest-link robustness
- Proactive guarantees
- Discourages misbehavior

Transparency

- Multi-eye-principle sanity checks
- Public logs



Scalability

- Aggregation
- Communication trees
- Sign: O(log n) (8000 nodes, ~2 sec)
- Verify: O(1)

Security / Transparency Levels

Weakest

Strongest

Level 0

- Traditional authorities
- No witness co-signing
- No public log(s)

Level 1

- Witness co-signing
- Public log(s)
- Check nothing
- Generic
- Easy to upgrade existing authorities

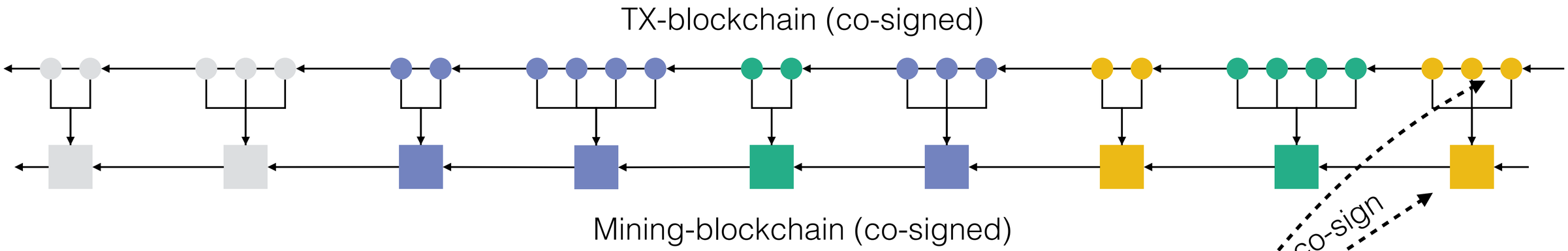
Level 2

- Witness co-signing
- Public log(s)
- Check authority statements
- E.g., reproducible builds for software updates

Level 3

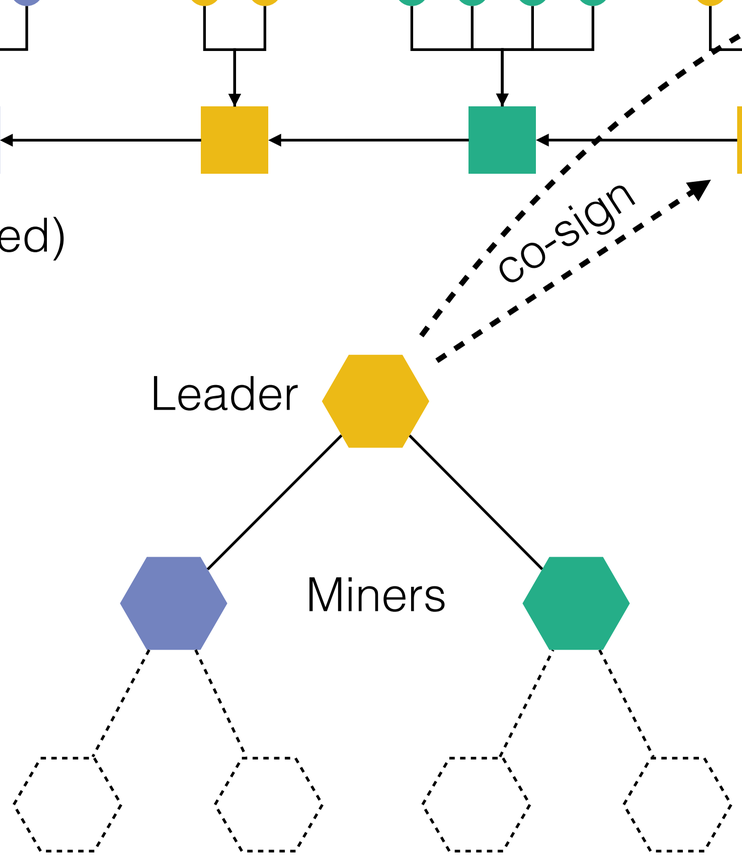
- Witness co-signing BFT consensus
- Public log(s)
- Check consistency of distributed processes
- E.g., blockchain extension in crypto-currencies

Scalable Strongly Consistent Blockchains



ByzCoin

- Non-probabilistic BFT consensus
- Scalable (1000+ nodes)
- Low latency (< 20 sec)
- High throughput (700+ TPS)
- Permissioned and permissionless

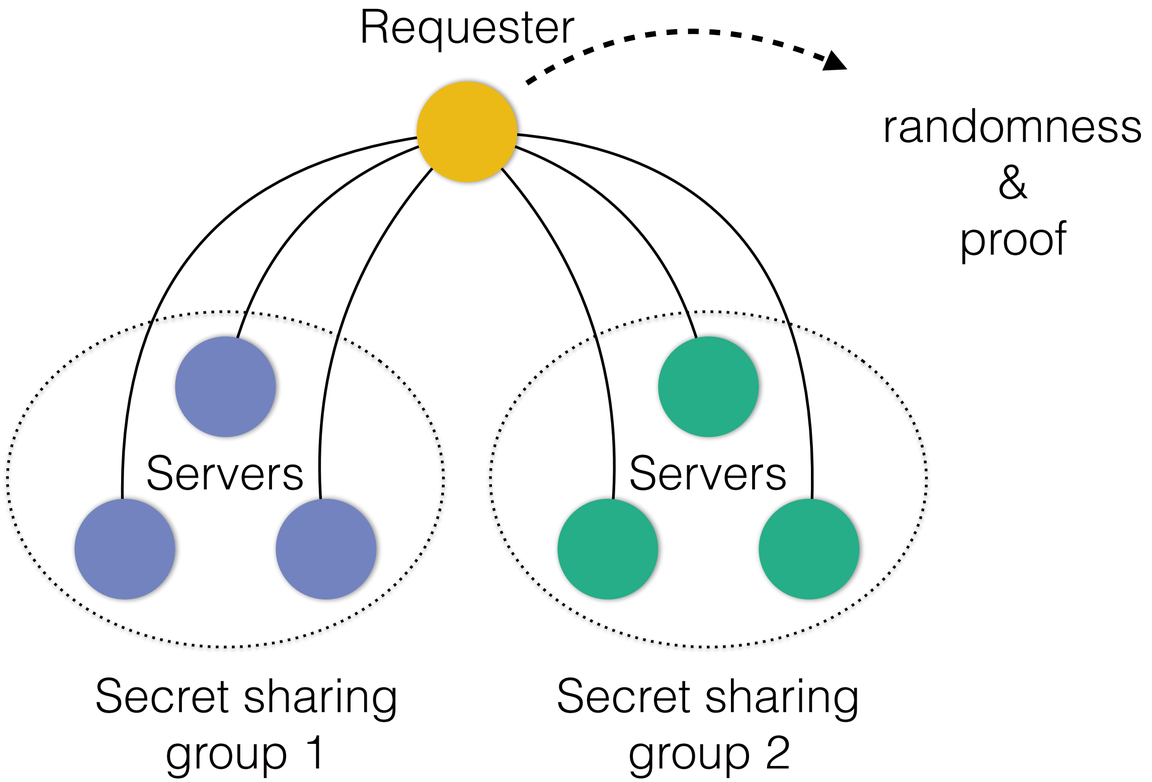


Mining cothority = Consensus group

Scalable Bias-Resistant Distributed Randomness

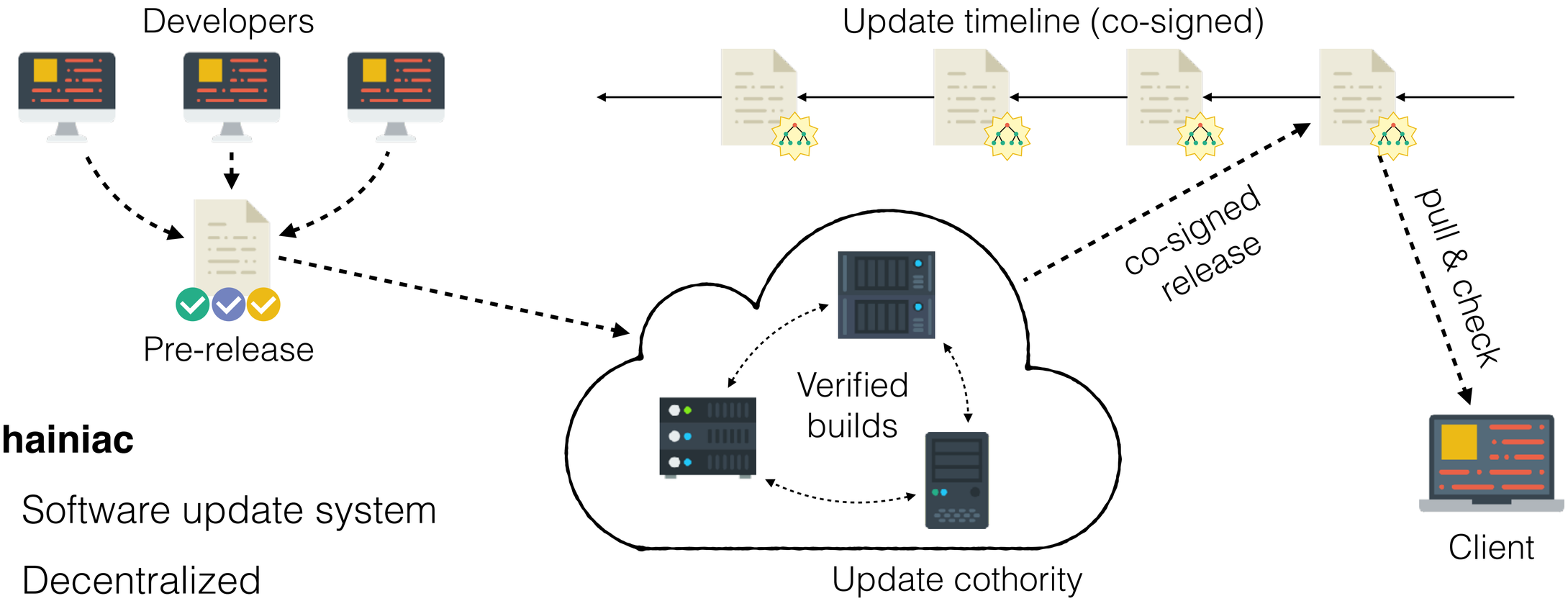
Rand{Hound, Herd}

- Randomness beacons
- Distributed
- Bias-resistant
- 3rd-party verifiable
- Scalable (1000+ nodes)
- Low latency



RandHound

Software Update Transparency



Chainiac

- Software update system
- Decentralized
- Co-signed update timeline
- Efficient source-to-binary verification

Further details

https://github.com/dedis/cothority

Thanks

@Daeinar