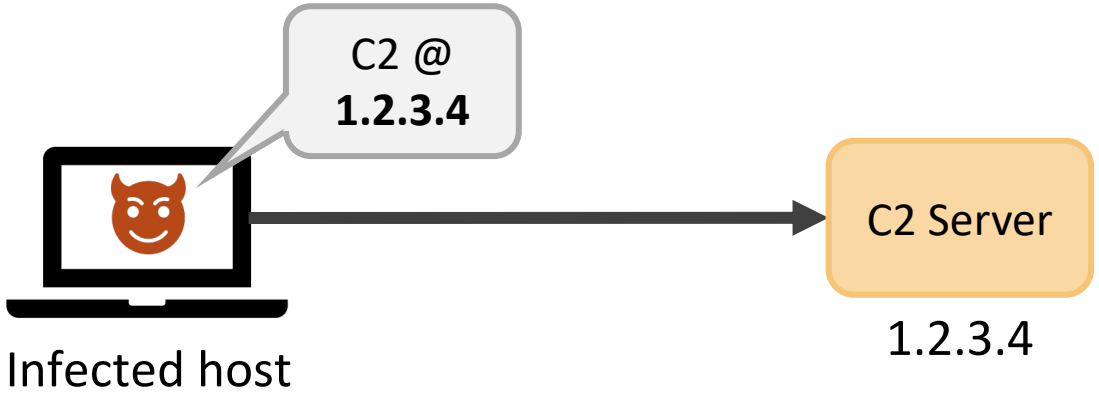
Challenges of Blockchain-Based Naming Systems for Malware Defenders

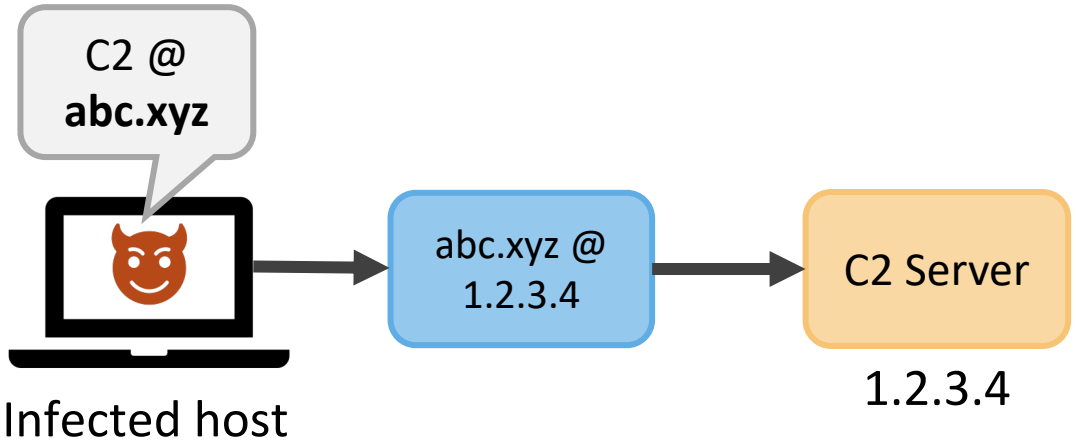
Audrey Randall*, Wes Hardaker†, Geoffrey M. Voelker*, Stefan Savage*, Aaron Schulman*

*University of California San Diego

†University of Southern California

Malware requires naming systems

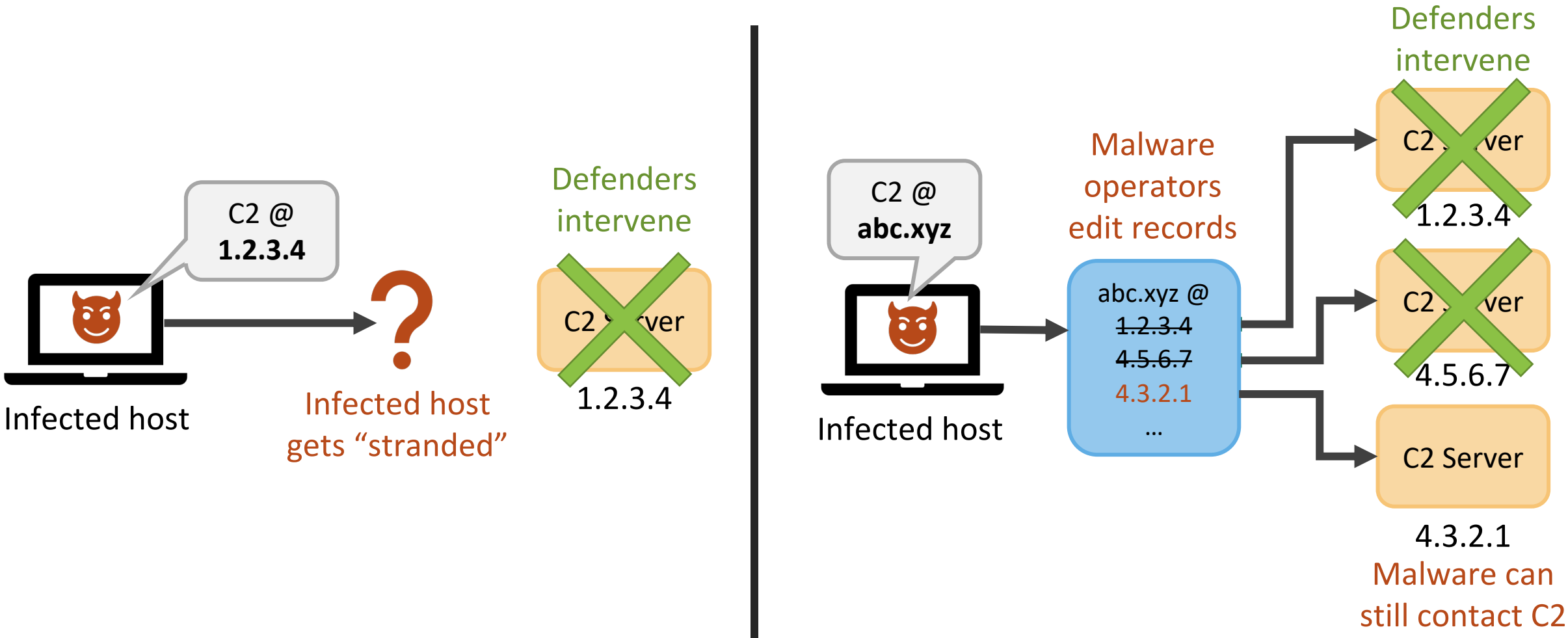




Without a naming layer

With a naming layer

Malware needs naming systems to reach C2



Desirable features for C2 naming system

Difficult to censor individual names

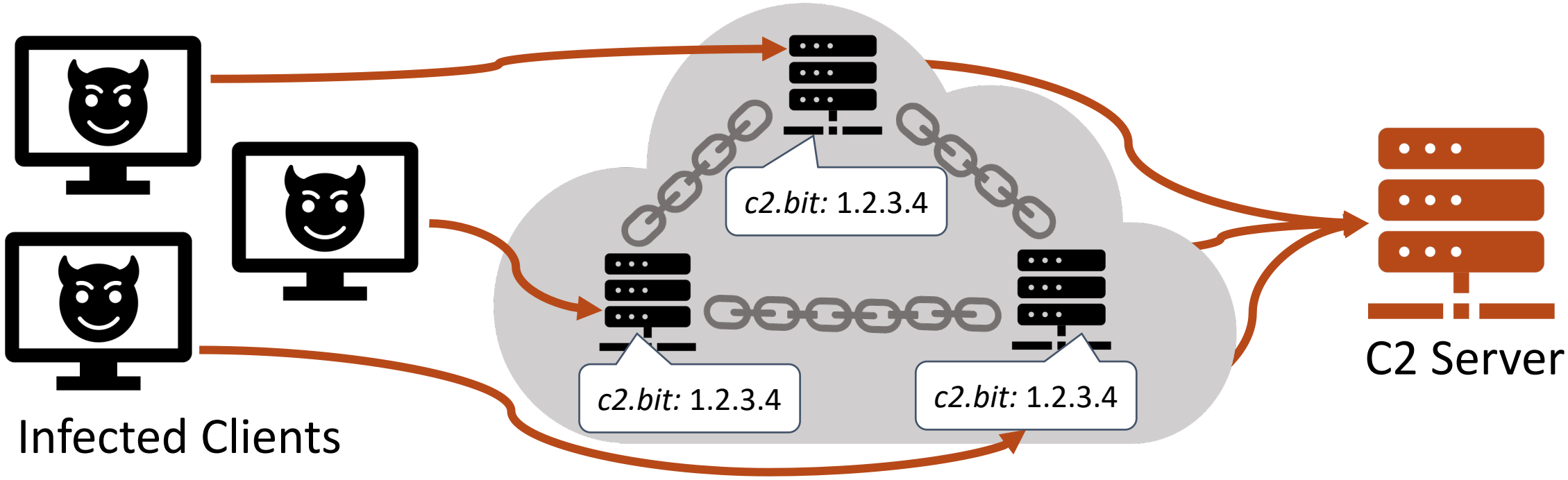
- No central authority with takedown capabilities.

Costly to take down entire system

- System must be useful to legitimate users.
- Takedown would create collateral damage.

“Blockchain Naming Systems” might have both properties?

What's a "Blockchain Naming System" (BNS)?



DNS vs. BNS as C2 naming systems

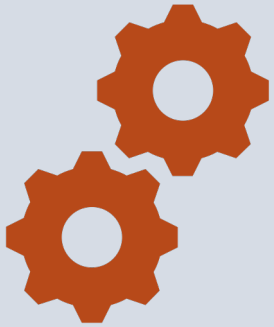
DNS

- **Critical.** Never blocked wholesale.
- Subject to **hierarchy of authorities**
  - Registrars
  - Registries
- Vulnerable to takedowns
- Single legal entity can perform an intervention.

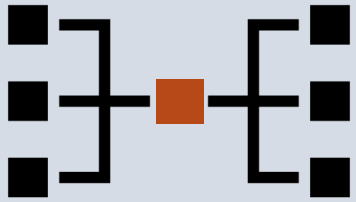
BNS

- **No central authority.**
  - Cannot take down record without its private key
- Growing blockchain popularity
  - Blocking access -> **collateral damage.**
- Already used by malware in the wild

Our Research Questions



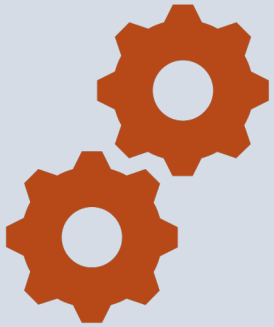
How do these systems work?



Do ecosystem bottlenecks exist where interventions might be possible?

Which BNS systems are optimal for malware?

Our Research Questions



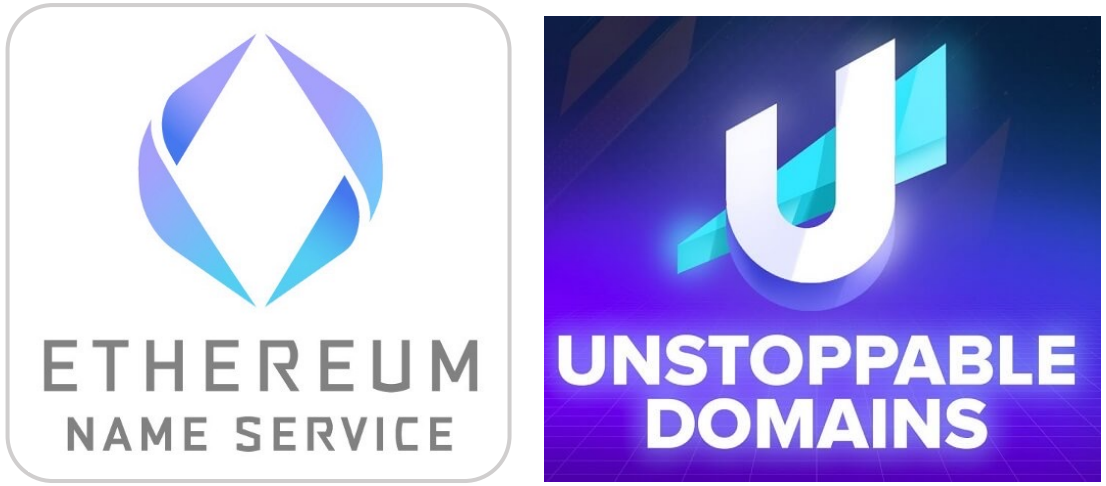
How do these systems work?

Do ecosystem bottlenecks exist where interventions might be possible?

Which BNS systems are optimal for malware?

BNS comes in two categories

BNS built on
naming-specific blockchains



BNS built on
general-purpose blockchains

BNS name resolution

BNS names use alternate TLDs.

Can’t be resolved by DNS. Instead, resolution requires:

- Proxies
- Browser extensions
- Built-in browser support

Name system	TLDs	Proxies
Namecoin	.bit	BDNS (defunct), PeerName
Emercoin	.lib, .bazar, .coin, .emc	friGate, PeerName, OpenNIC
Handshake	*any string*	hns.to, NextDNS, HDNS.io, BobWallet extension, LinkFrame extension
ENS	.eth	eth.link, eth.limo
Unstoppable	.crypto, .blockchain, .bitcoin, .coin, .nft, .wallet, .888, .dao, .x, .zil	Brave browser, Opera browser, Unstoppable browser, Unstoppable extension, Infura

Namespace Collisions in Alternate Roots

BNS vs. ICANN

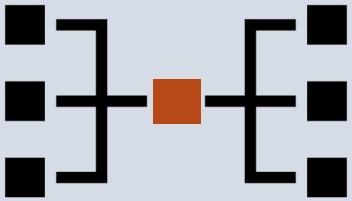
- `.music` alt-TLD bought by Handshake customer, later introduced by ICANN
- Drama and legal threats ensue

BNS vs BNS: no coordination

- Unstoppable Domains removed support for `.coin:` collides w/ Emercoin.
- Handshake `.wallet` collides with Unstoppable Domains

Our Research Questions

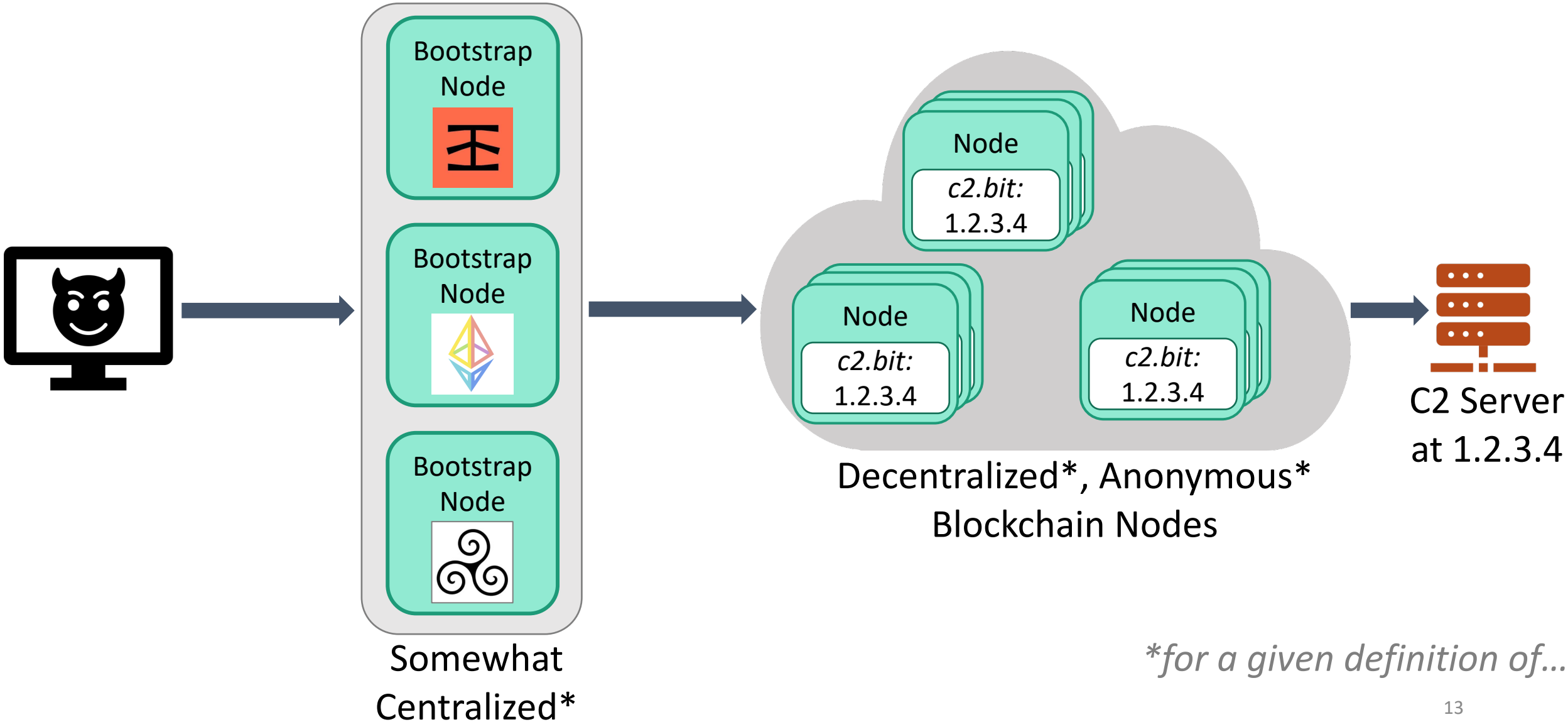
How do these systems work?



Do ecosystem bottlenecks exist where interventions might be possible?

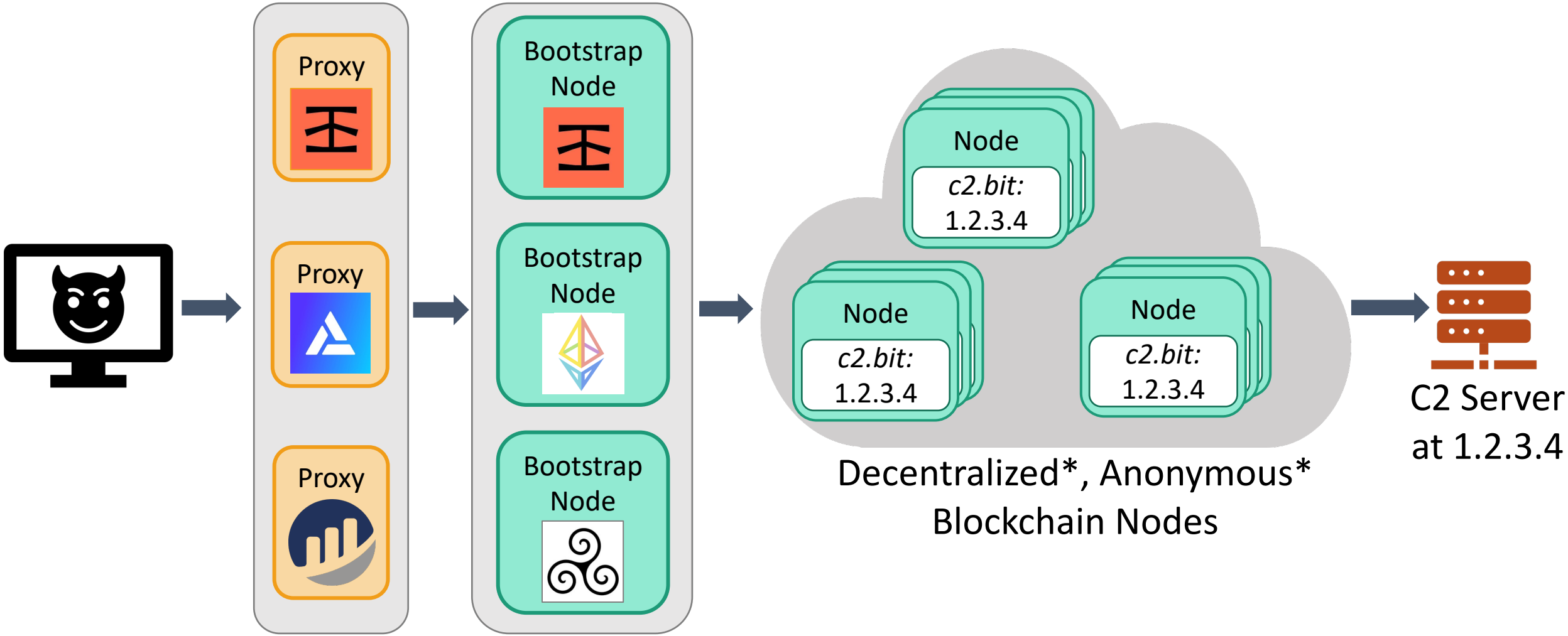
Which BNS systems are optimal for malware?

How malware uses a blockchain naming system



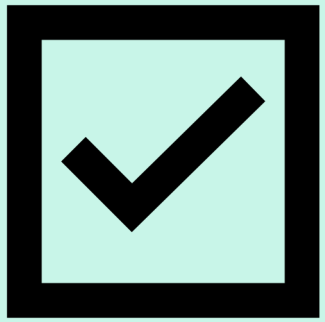
**for a given definition of…*

How malware uses a blockchain naming system



**for a given definition of…*

Types of Interventions

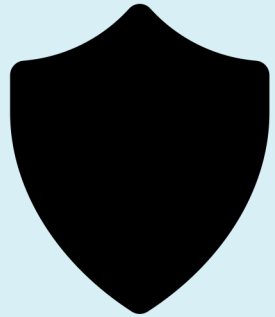


Blocklist

*Request must cross machine with **capability & willingness** to implement a blocklist.*

Temporary Restraining Order (TRO)

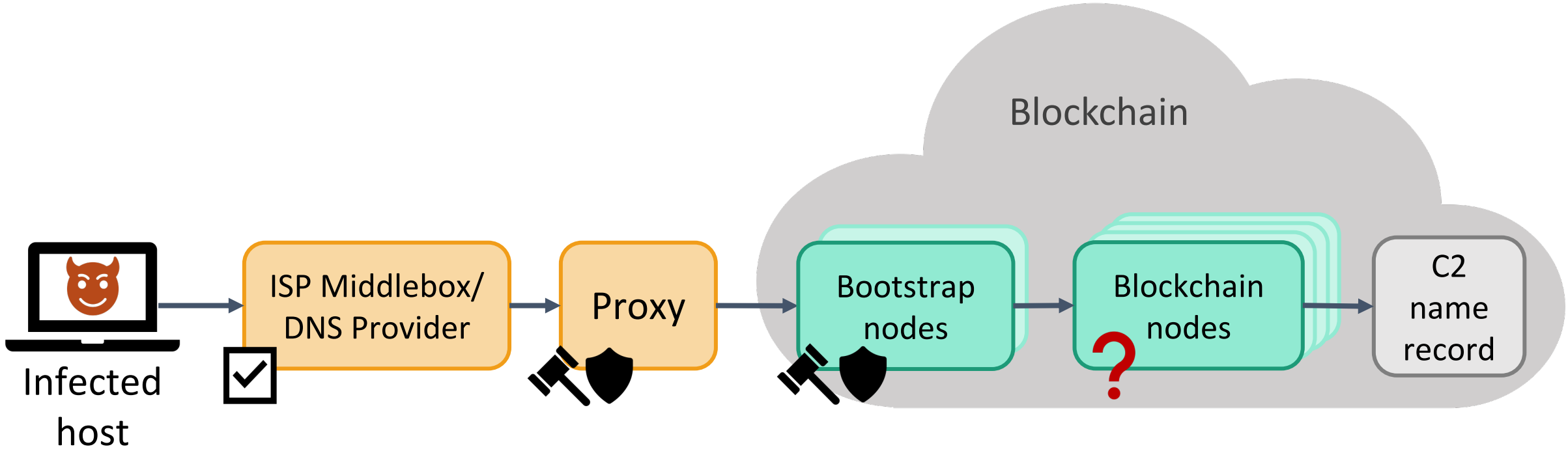
*Grants **legal authority** to order **intermediaries** (registrar, proxies) to deny service to customer.*



Host Seizure

***Physical seizure** or **Storage Communications Act warrant** to shut down and image the device.*

Potential Locations for Interventions



Interventions

Blocklist *TRO* *Host seizure*

Our Research Questions

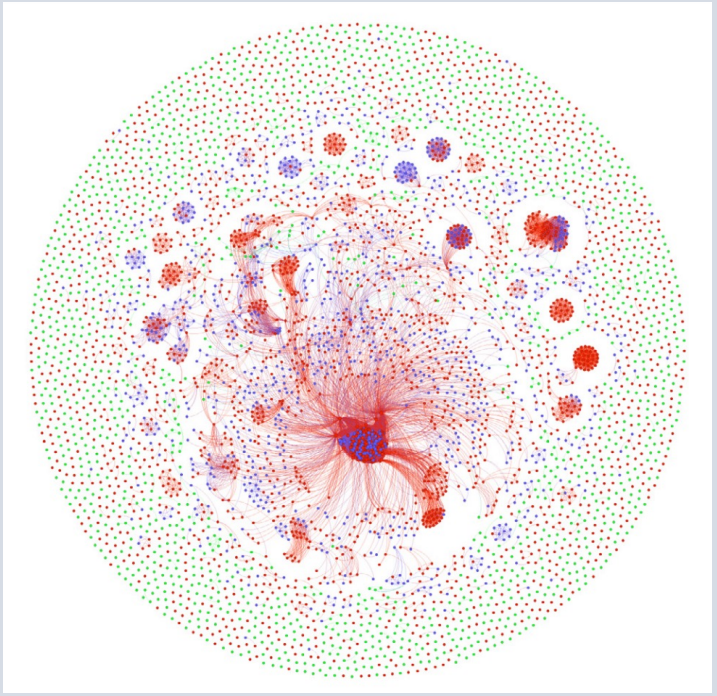
How do these systems work?

Do ecosystem bottlenecks exist where interventions might be possible?

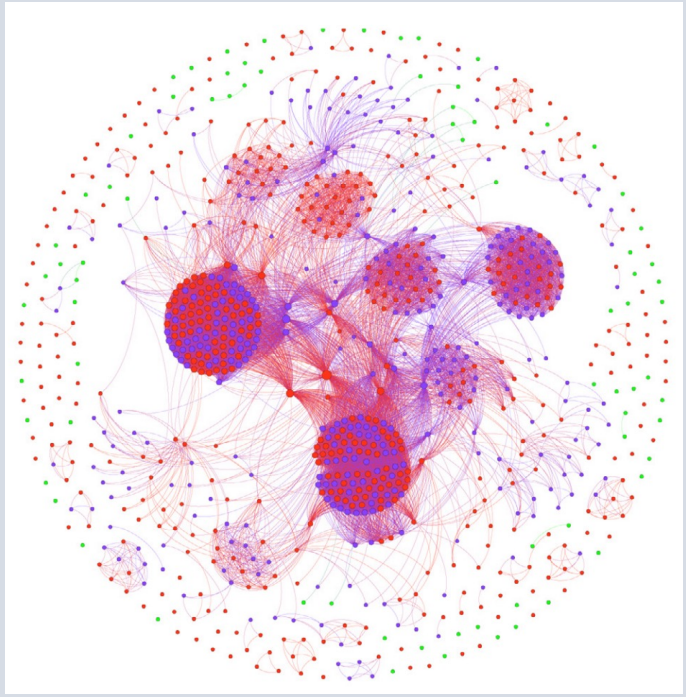
Which BNS systems are optimal for malware?

BNS on naming-specific blockchains: Namecoin/Emercoin

Namecoin



Emercoin



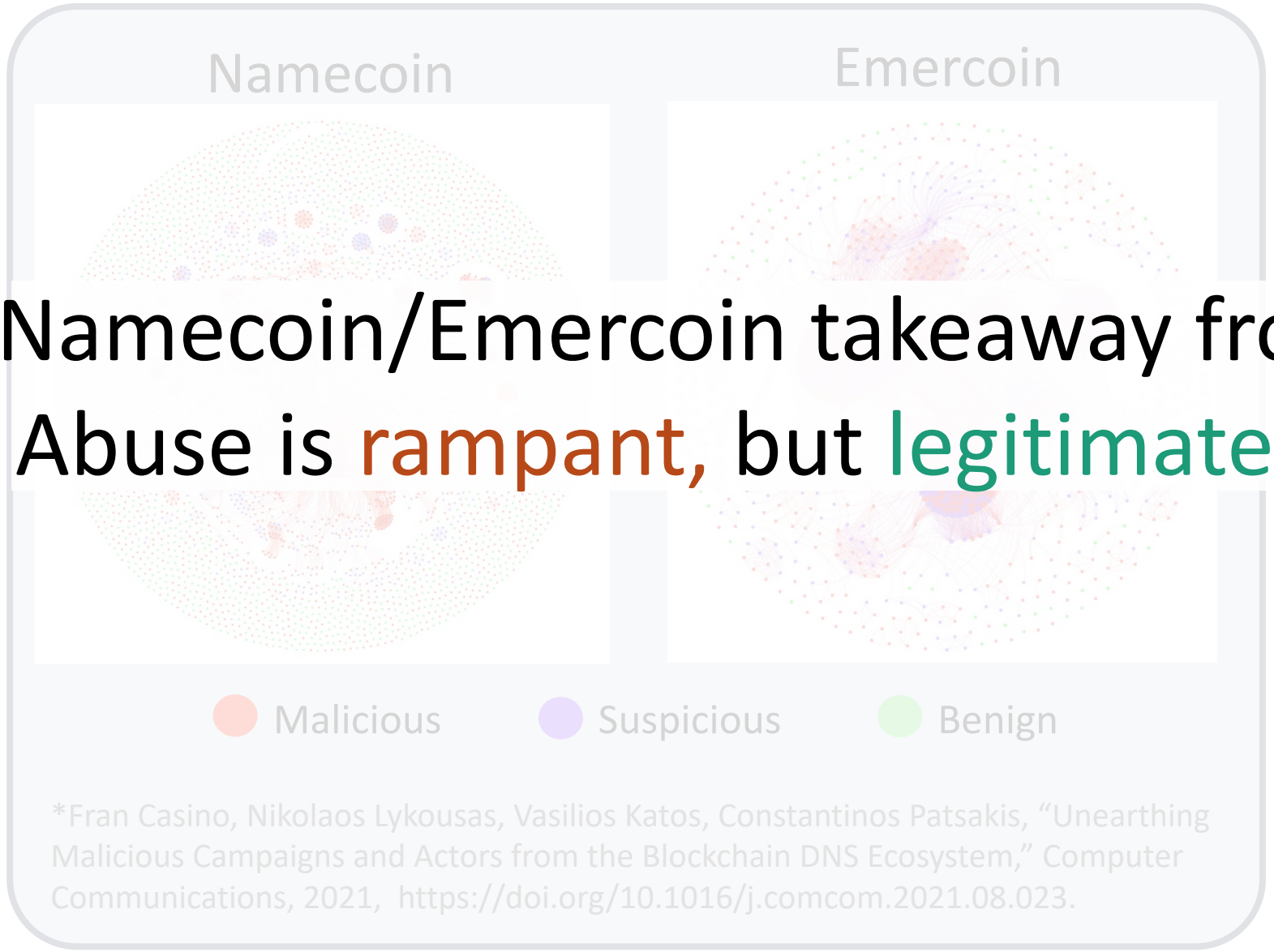
Malicious Suspicious Benign

*Fran Casino, Nikolaos Lykousas, Vasilios Katos, Constantinos Patsakis, “Unearthing Malicious Campaigns and Actors from the Blockchain DNS Ecosystem,” Computer Communications, 2021, https://doi.org/10.1016/j.comcom.2021.08.023.

Findings from **prior work***

Node: IP address. Edge: wallet address, email address, domain.

BNS on naming-specific blockchains: Namecoin/Emercoin



*Fran Casino, Nikolaos Lykousas, Vasilios Katos, Constantinos Patsakis, "Unearthing Malicious Campaigns and Actors from the Blockchain DNS Ecosystem," Computer Communications, 2021, https://doi.org/10.1016/j.comcom.2021.08.023.

Findings from

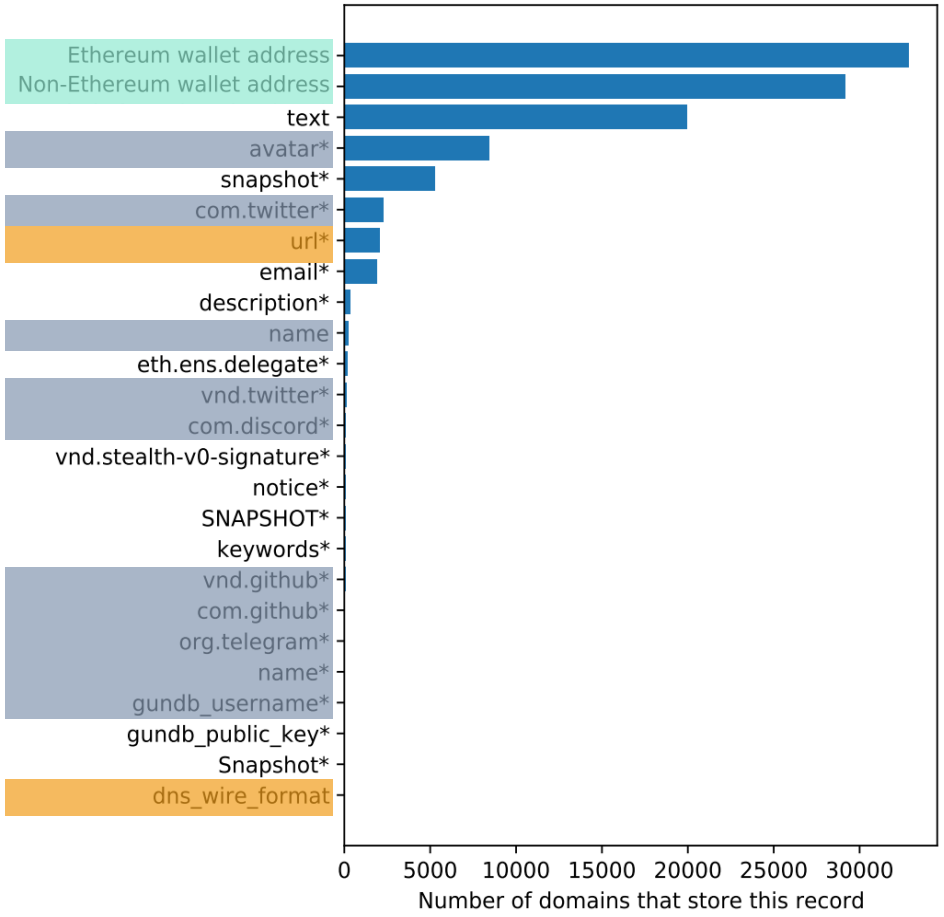
Node: IP address, Edge: wallet

Abuse is rampant and possibly provides most of the usage of these systems!

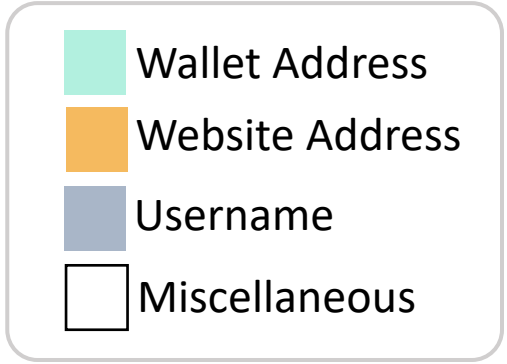
Namecoin/Emercoin takeaway from Casino et al.:

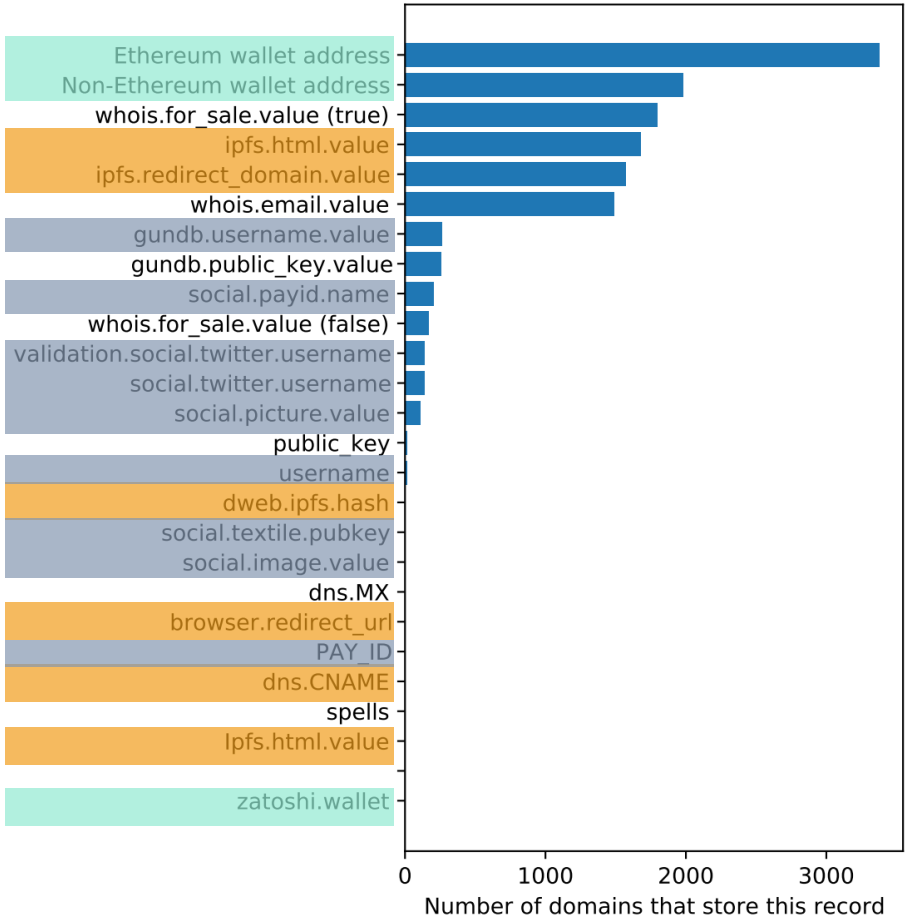
Abuse is rampant, but legitimate use is very low.

BNS on general-purpose blockchains: ENS/Unstoppable Domains



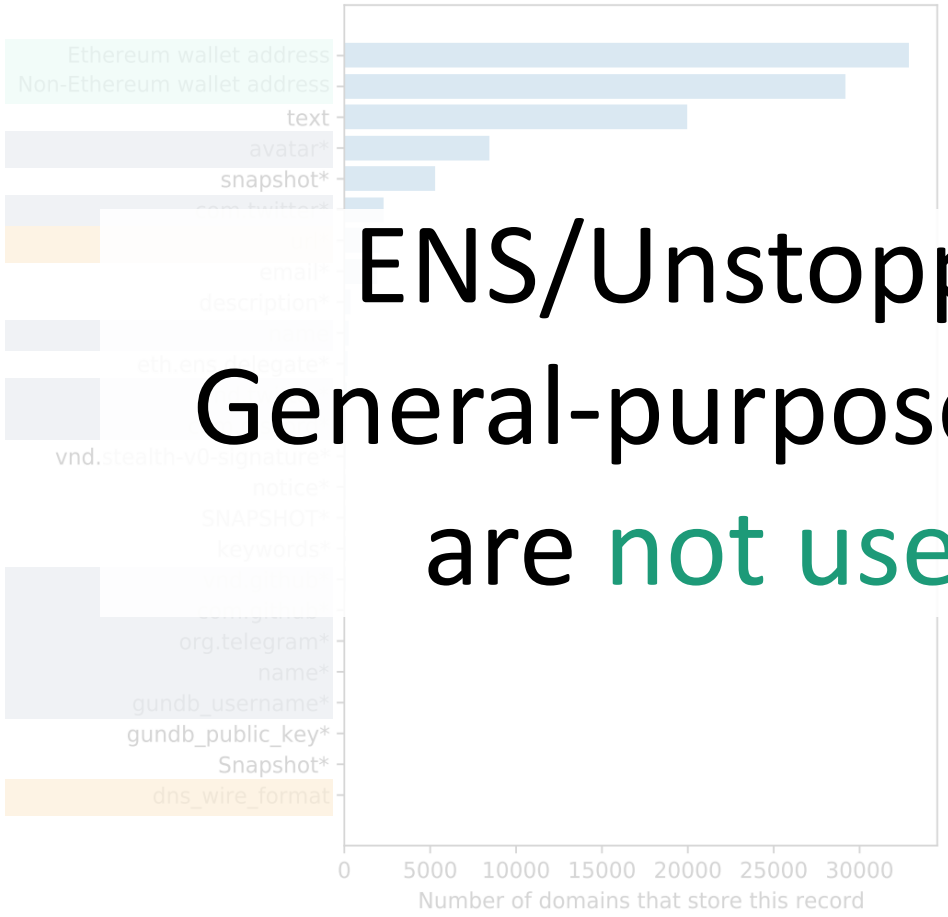
Ethereum Name Service (ENS) Name Records



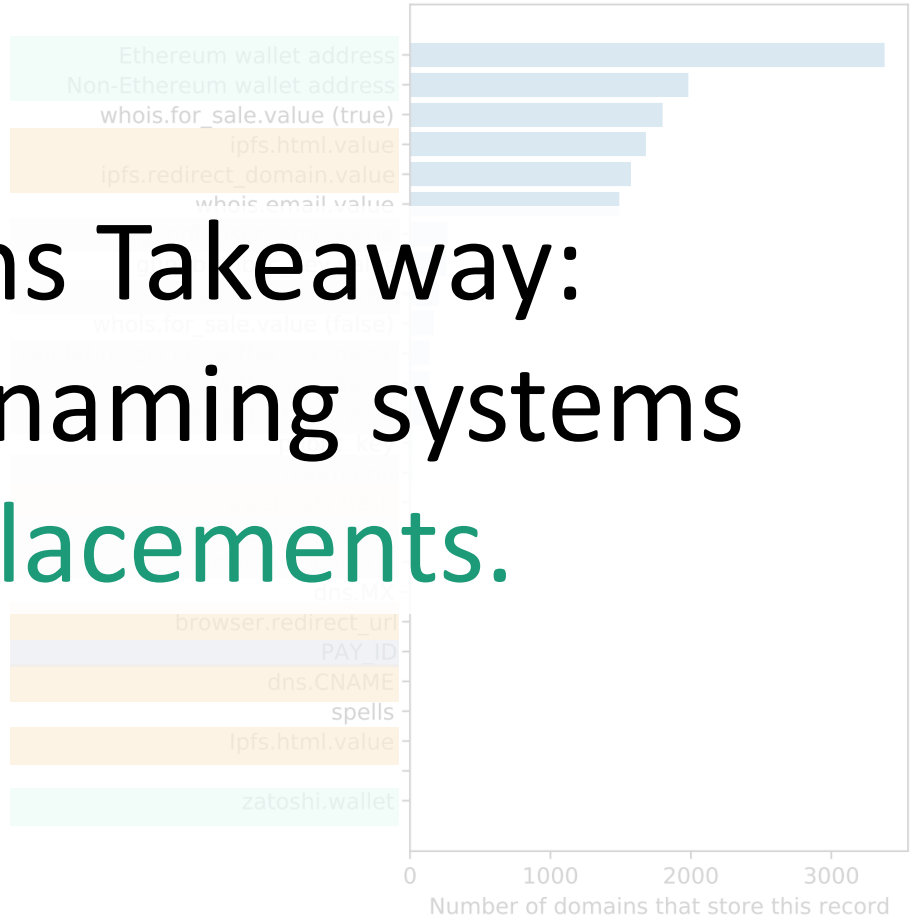


Unstoppable Domains Name Records

BNS on general-purpose blockchains: ENS/Unstoppable Domains



Ethereum Name Service (ENS) Name Records



Unstoppable Domains Name Records

ENS/Unstoppable Domains Takeaway: General-purpose blockchain naming systems are not used as DNS replacements.

Low abuse on general-purpose BNS?

ENS/Unstoppable show no signs of malware use

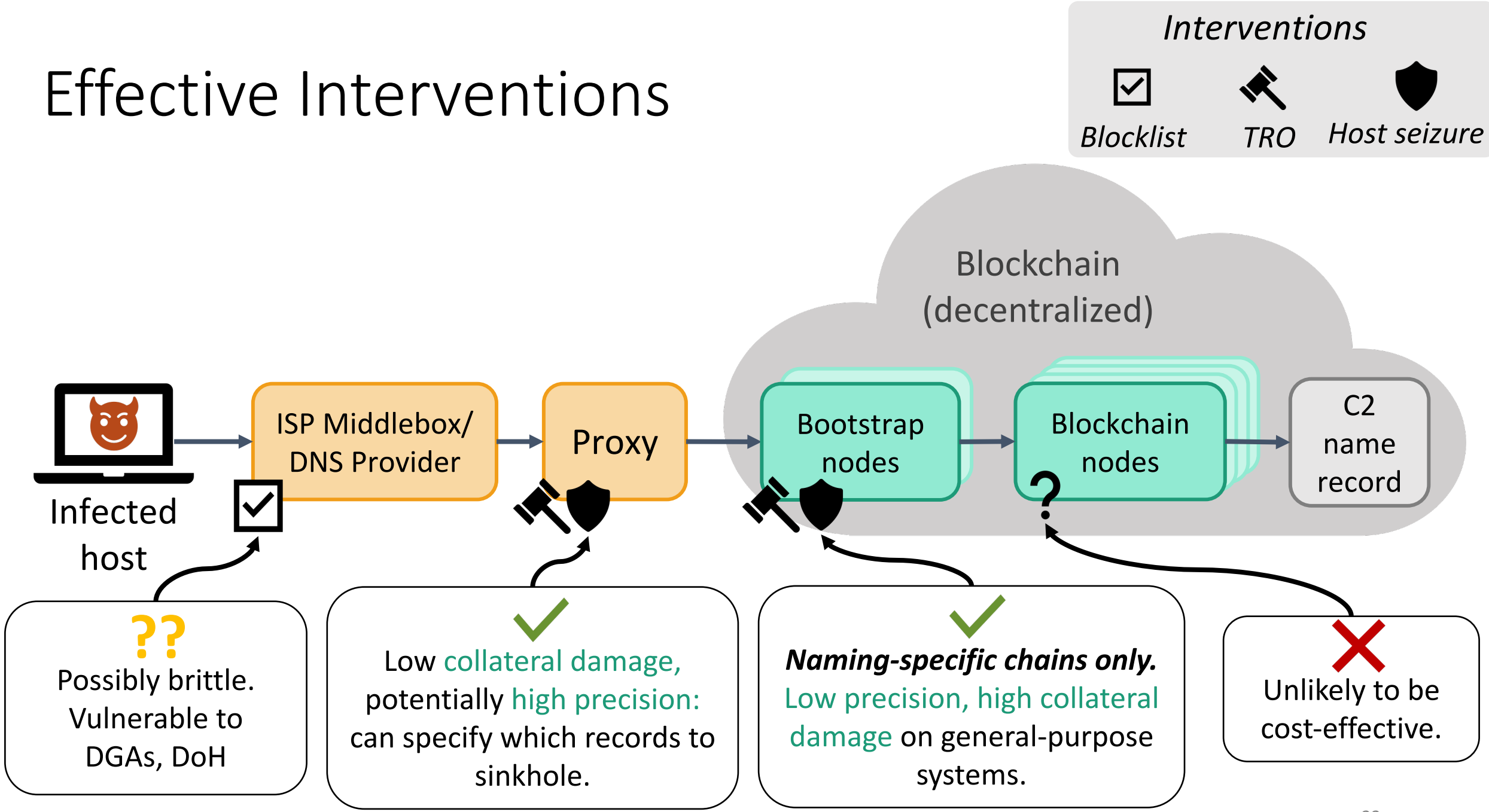
- General-purpose chains -> higher licit adoption -> more collateral damage if defenders take it down.
- Why no malware adoption?

General-purpose BNS is **too expensive!**

- Names are ~10$ minimum
- Transaction (“gas”) fees can be ~$10-$140

Naming-specific BNSes are cheap (relative to DNS).

Effective Interventions



Prior Interventions That Worked

OpenNIC (alternate root) ceases supporting `.bit`

- Spamhaus, Malwarebytes blocklisted OpenNIC resolvers.
- Community voted to remove `.bit` support.

“Blockchain-DNS.info” proxy takedown

- Some proxy endpoints sinkholed, more blocklisted by Spamhaus.
- Proxy moved to bulletproof provider, but is now entirely defunct.

Conclusion

BNS is not an insurmountable threat.

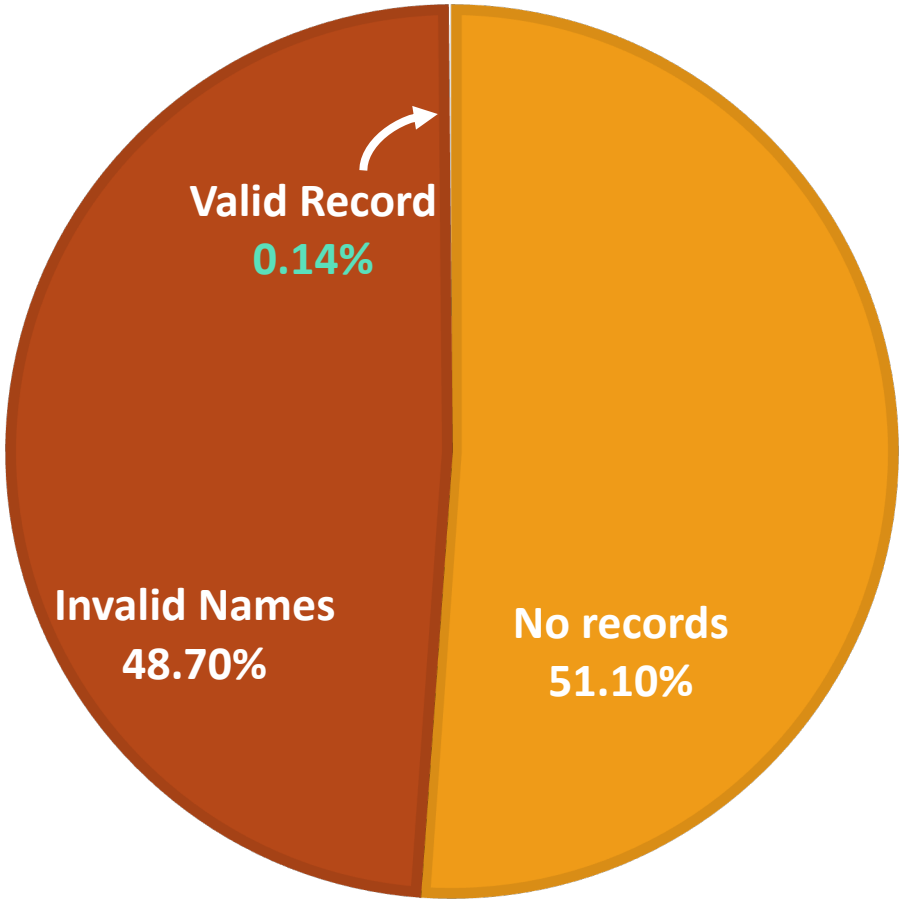
- Centralized chokepoints still exist
- Low licit use of Namecoin/Emercoin: can block entirely.
- High licit adoption but low malicious use of Handshake/ENS/Unstoppable Domains
  - Malware unlikely to adopt unless fees decrease!

BNS must become widely adopted to become dangerous:

- Name management must be easy
- Transaction fees must be low
- Browsers must adopt the BNS system natively

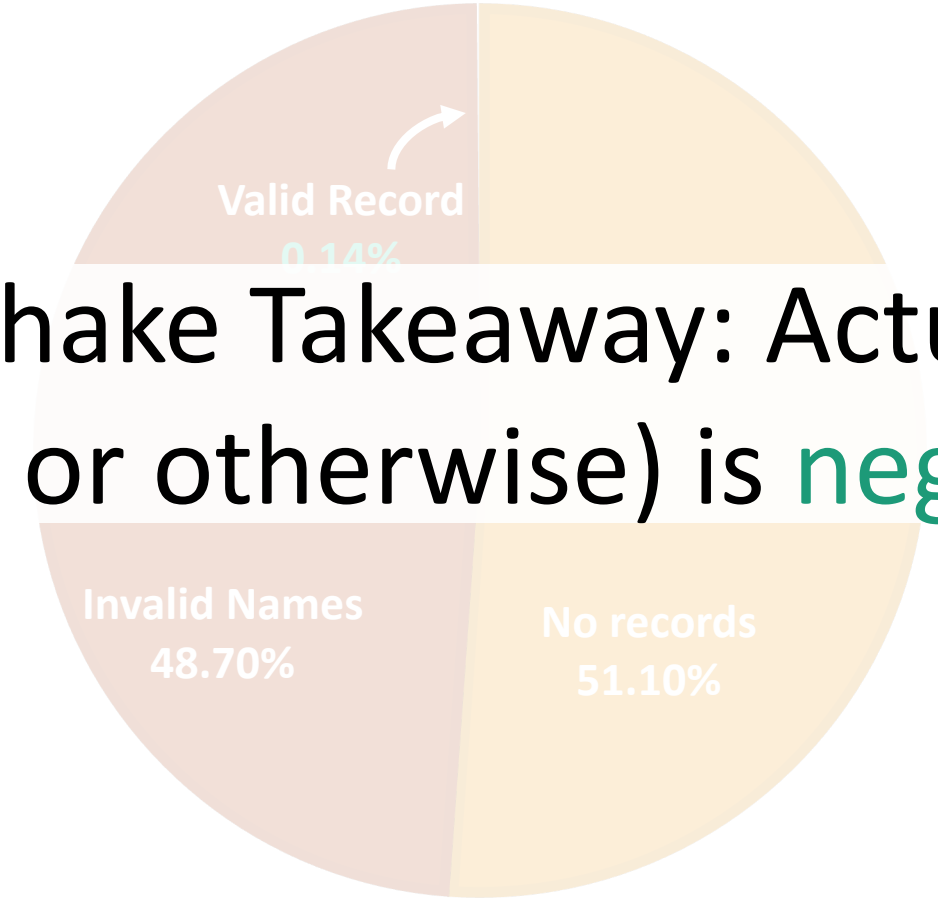
Extra slides

BNS on naming-specific blockchains: Handshake



Types of records stored in the Handshake Name System

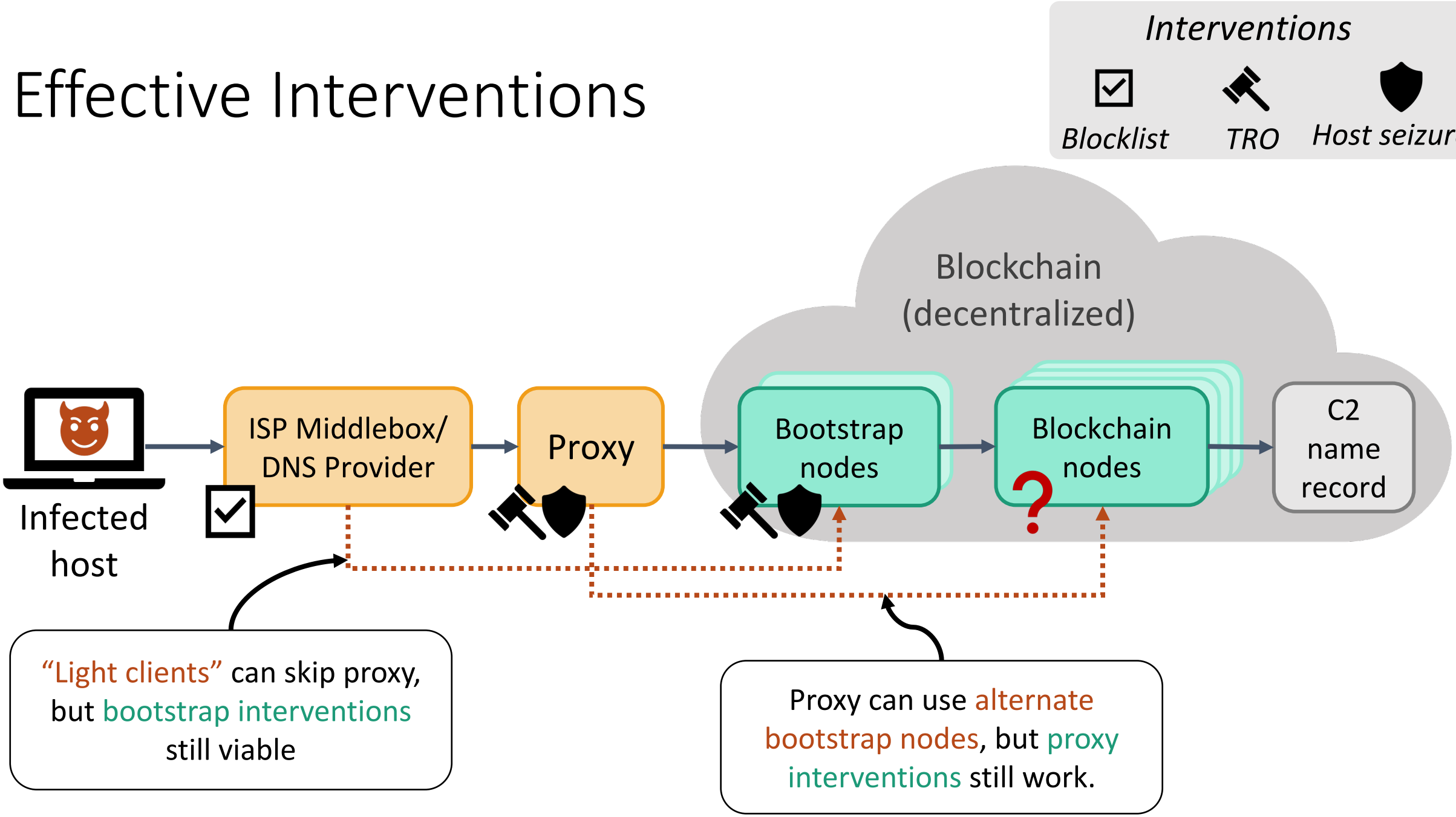
BNS on naming-specific blockchains: Handshake



Types of records stored in the Handshake Name System

Handshake Takeaway: Actual use (abuse or otherwise) is negligible.

Effective Interventions



Measurements of Name Resolution Queries

- BNS queries “leak” to the DNS root servers
- Unregistered names in general-purpose naming systems
  - No evidence of malware-related DGAs
- Unregistered names in naming-specific naming systems
  - Malware related, confirmed via VirusTotal and manual Googling
- Registered names in general-purpose naming systems
  - Very few names and requests per name
  - No names were in VirusTotal