



# Decentralized Domain Name System

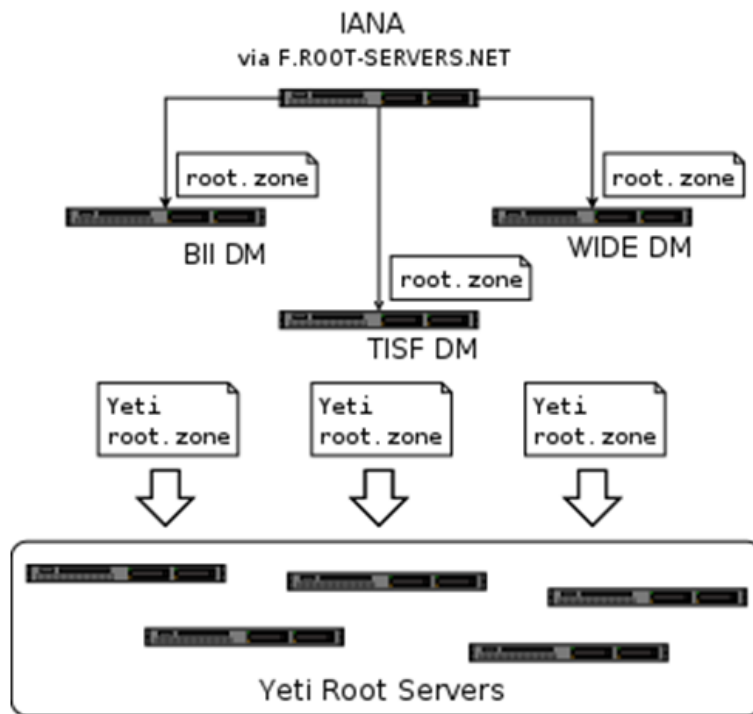
Yeti project phase-2

Li Zhen @ BII

2020/03/29

# Yeti phase-1 retrospection

## Three DMs setup and coordination

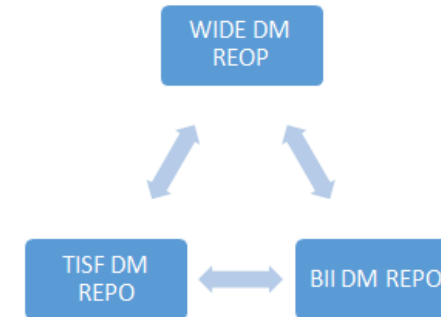


### Timing setting

DM	Time
BII	<i>hour + 00</i>
WIDE	<i>hour + 20</i>
TISF	<i>hour + 40</i>

Time of Fetching the zone

### Synchronizing



KSK, ZSK, server list,  
IANA serial number

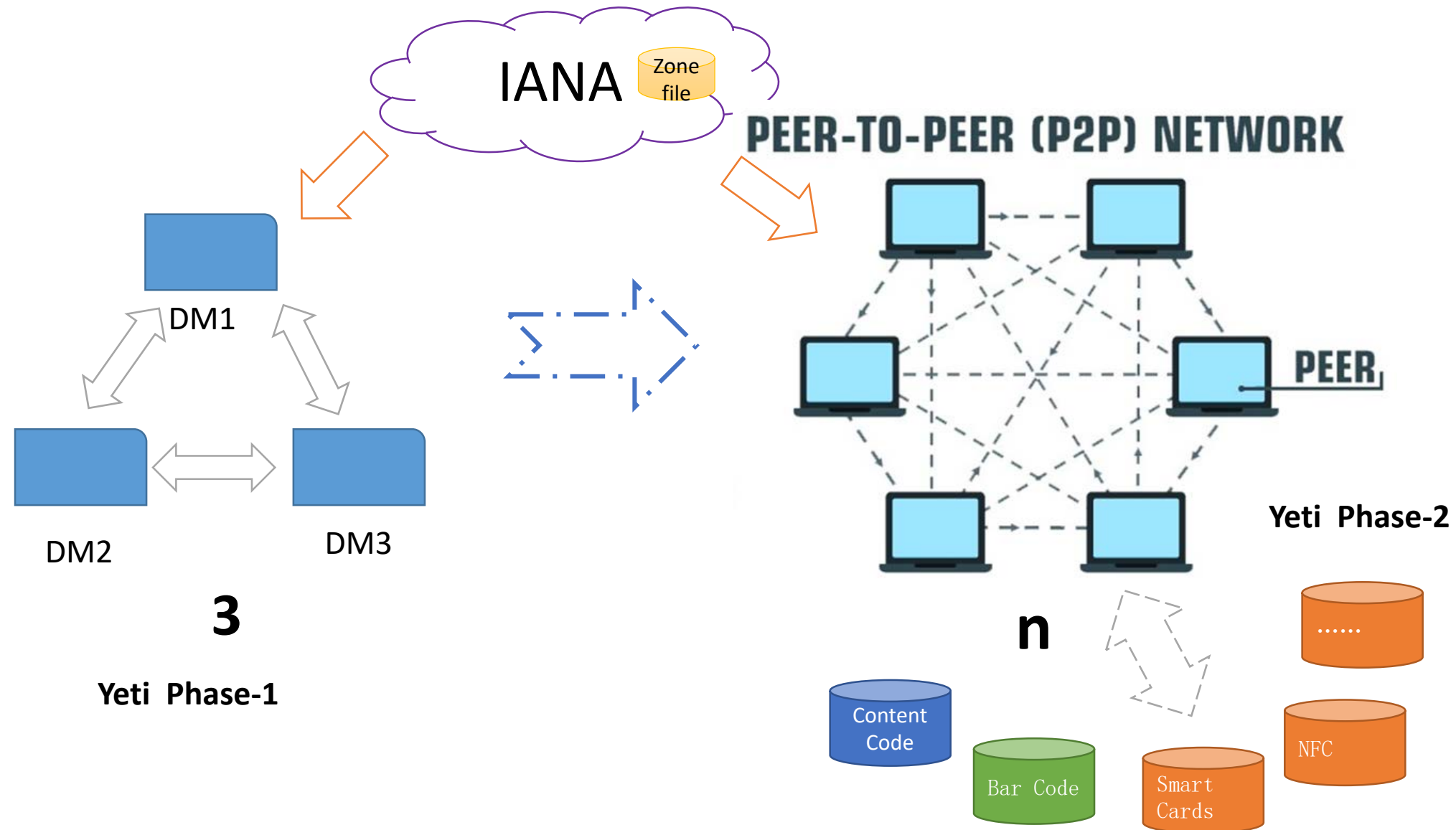
<https://github.com/BII-Lab/Yeti-Project/blob/master/doc/Yeti-DM-Setup.md>  
<https://github.com/BII-Lab/Yeti-Project/blob/master/doc/Yeti-DM-Sync.md>



# Yeti Phase-1 3 DMs Pros/Cons

- Pros
  - Redundancy: avoid single point of failure
  - Three root zone files
- Cons
  - Large DNSKEY size: more ZSKs
  - Zone transfer issue: AXFR/IXFR
    - Mixed RRSIGs from different DM ZSKs
- Operational issue
  - More DMs add possibility of failure points

# Decentralized--- base on P2P network



# Vision to the Yeti Phase-2 infrastructure

- **Equity:**

- The rights and obligations of all nodes are equal.

- **Robustness:**

- No single entity can cause significant damage to the infrastructure

- **Trust:**

- Infrastructures become more trustable, which can improve efficiency of networked services

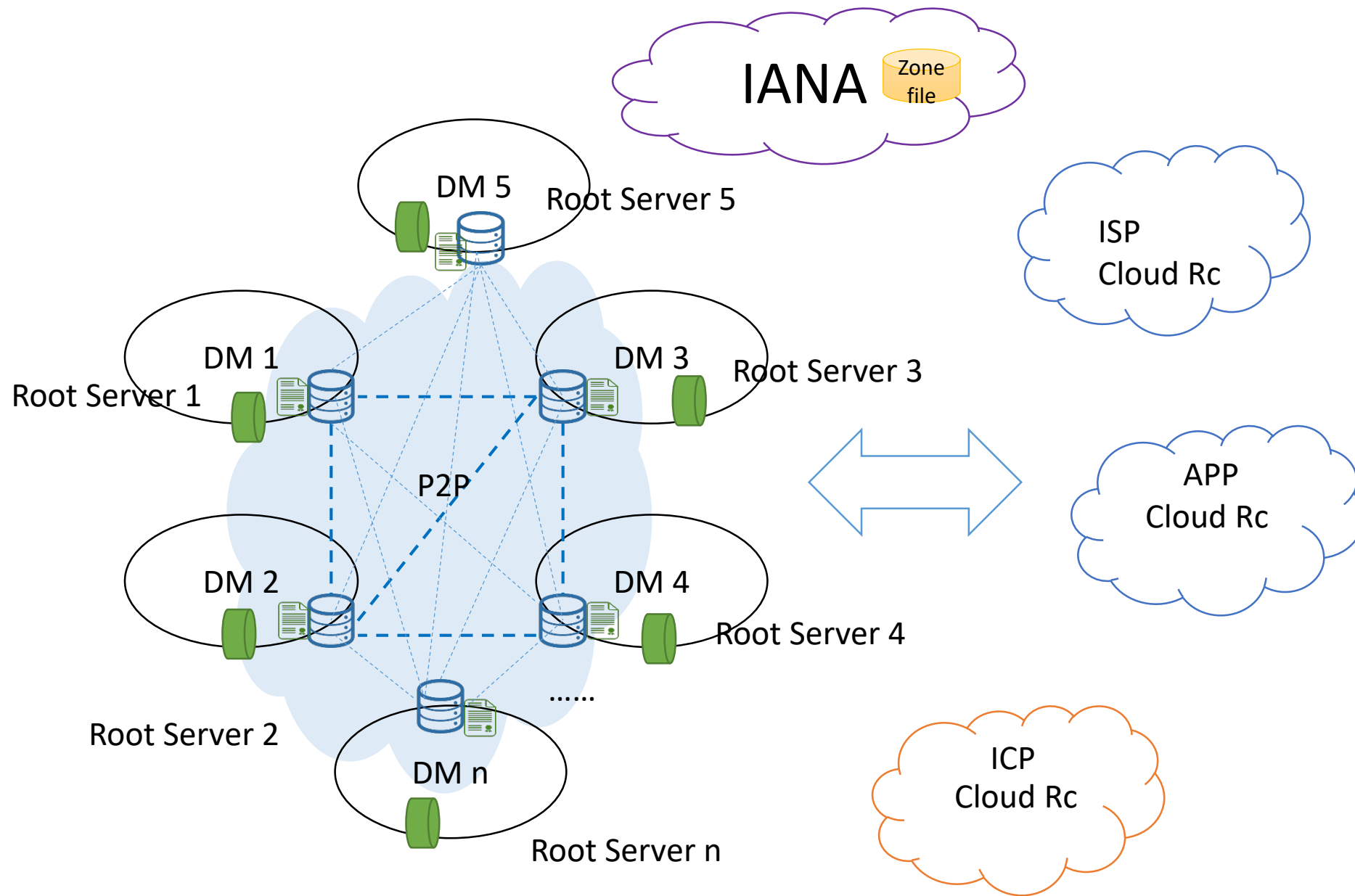
- **Innovation:**

- New industry like IOT domain name (APP/Content/Device Identity) can be tried on decentralized infrastructure.

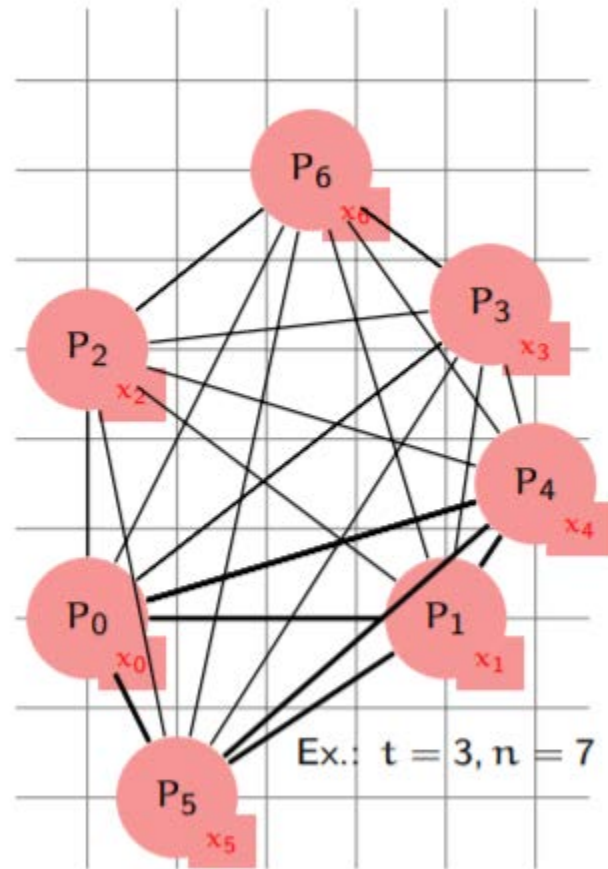


# Requirements

- Prerequisite
- Rule
- P2P network alliance
  - Smart contract
  - Mutual authentication
  - Automatic technical checks to Keep One name space (Zone file)
  - Participation and withdrawal mechanism

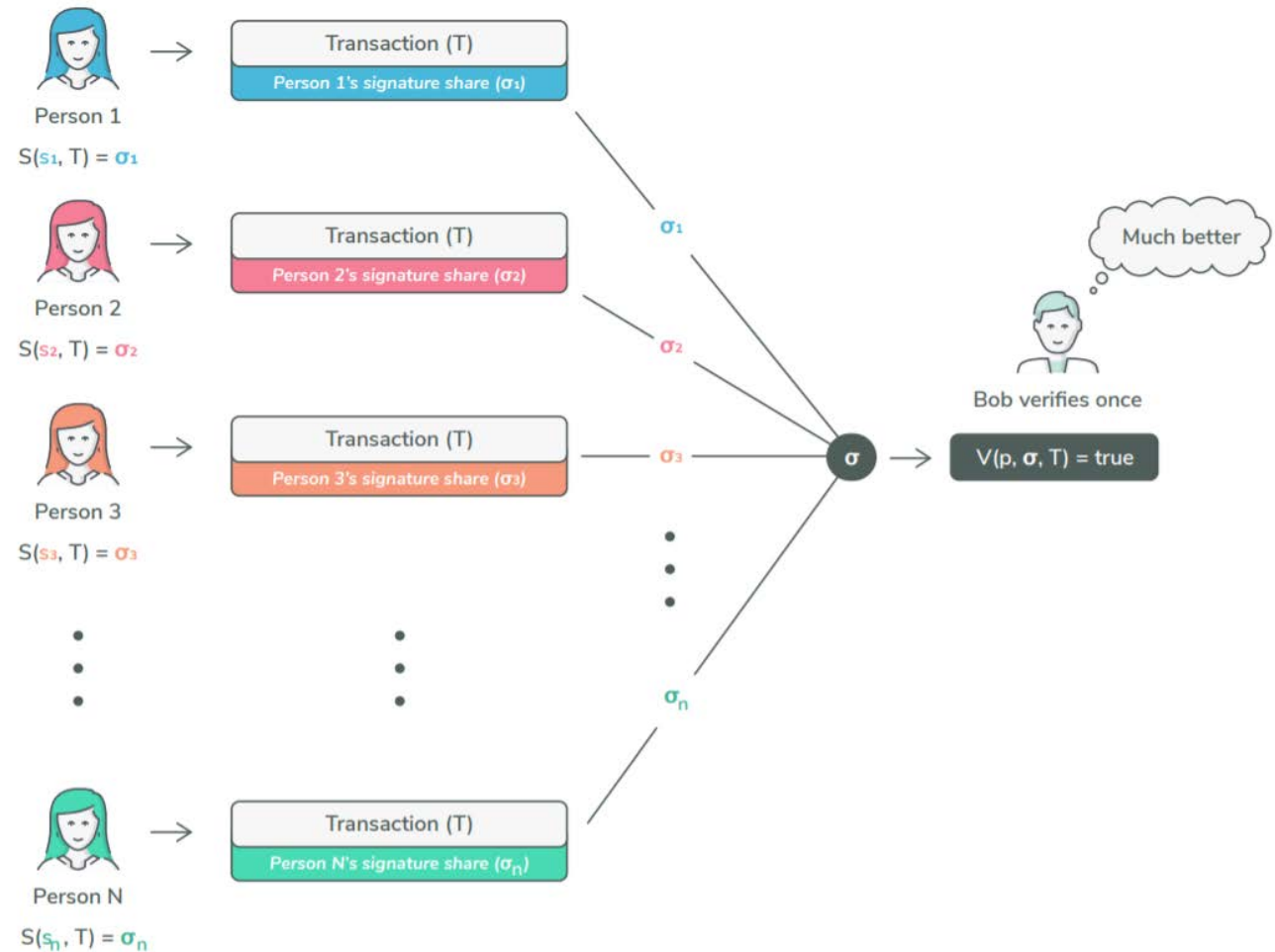


# Threshold Cryptography



shared secret and distributed algorithms with threshold  $t < n$

The system is functional even if not all  
The Shares retrieved





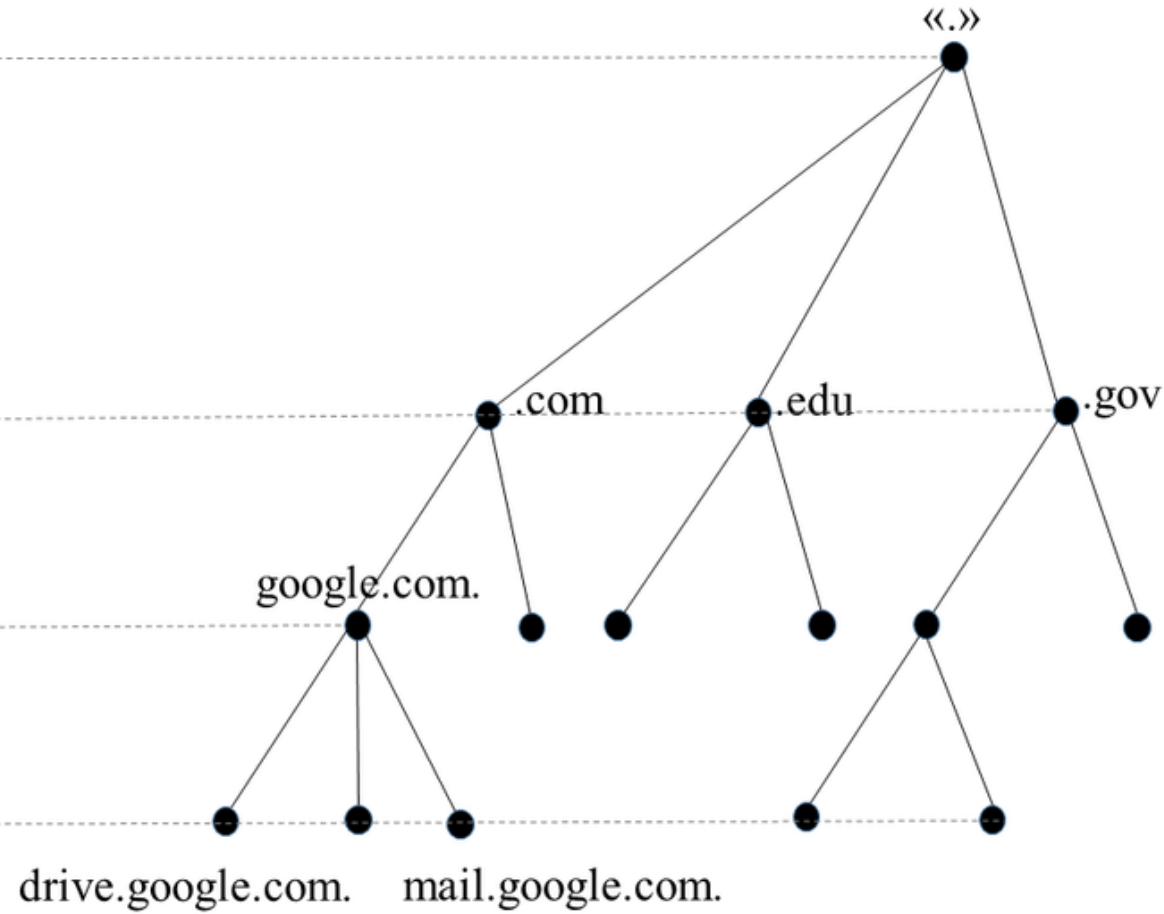


DNS-Root zone

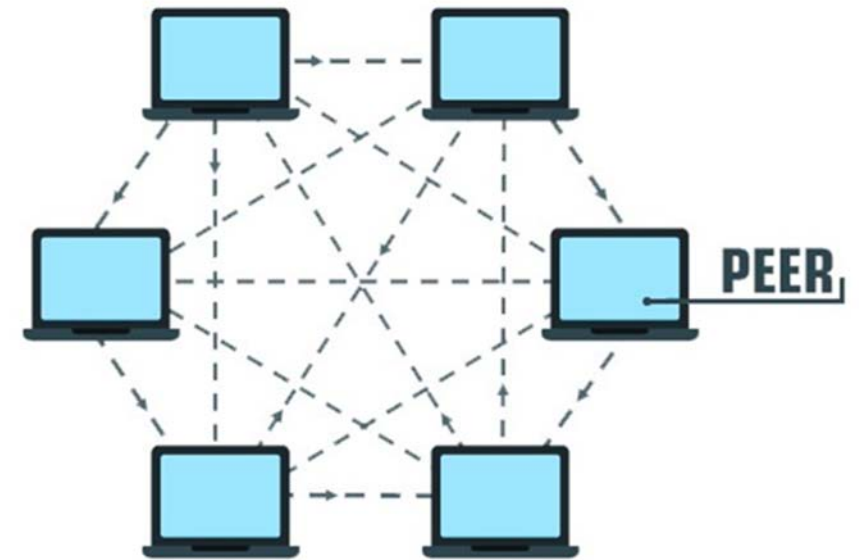
1<sup>st</sup> level zone

2<sup>nd</sup> level zone

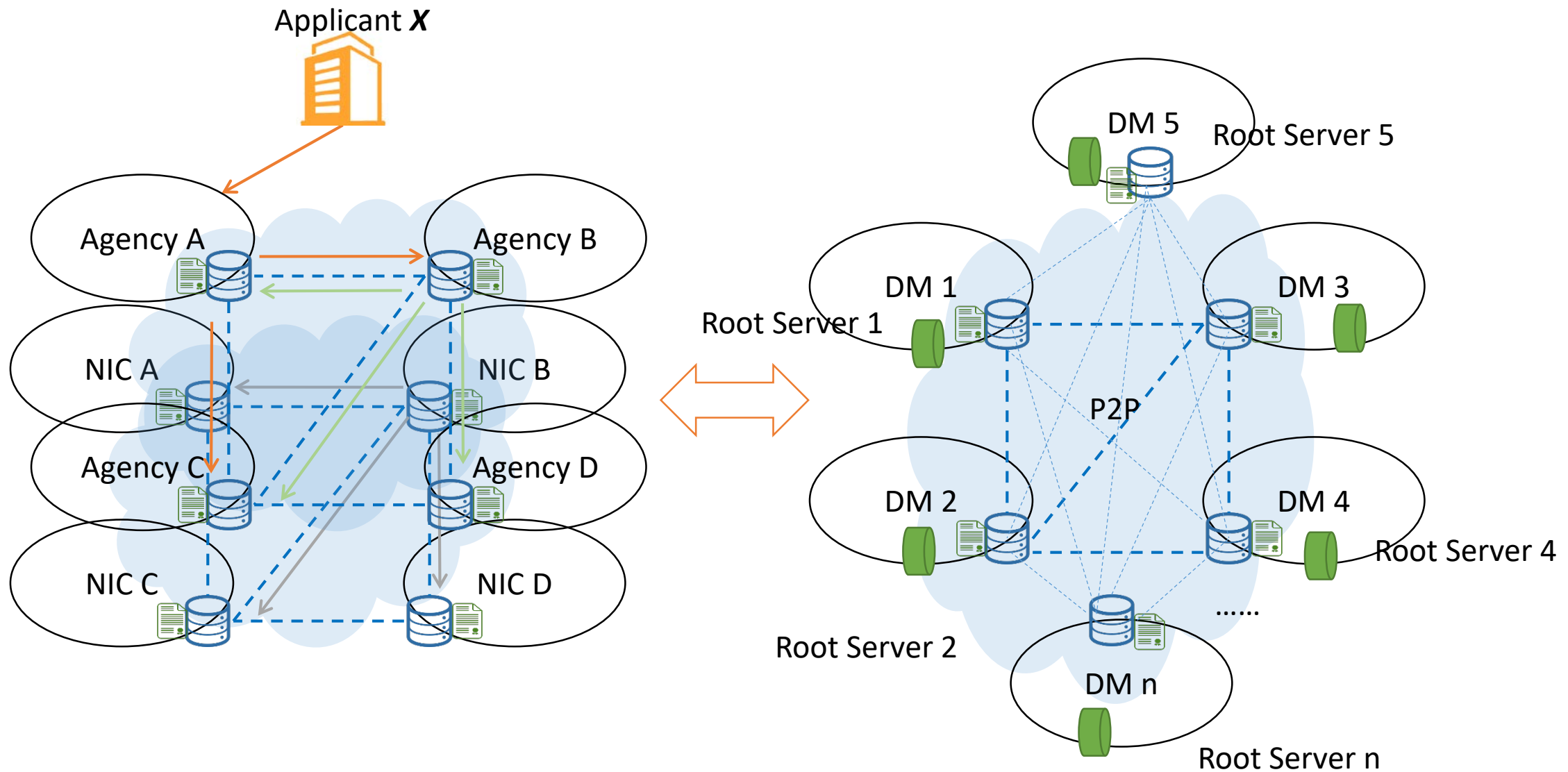
3<sup>rd</sup> level zone



## PEER-TO-PEER (P2P) NETWORK



# IOT/Content/video identification Trial



# Key work

- Refined P2P protocol
- Methodology
  - Design /Prototype/ Test/ Refinement
- What the number  $n$  should be when do test
  - $n=3$ /  $n=25$ /  $n=1000$  or bigger
- Compare with the Existing on Security and efficiency
  - Performance/latency/Accuracy
  - DDOS Anti-attack and other threats

# Challenge

- Consensus algorithms for specific scenarios
- Interaction and interoperability with existing DNS authoritative and recursive servers in DNSSEC context
- Signing scheme among a group of signers in decentralized communication settings
- Deployment and operation of more actual implementations in Yeti Test bed

# Organization

- Yeti DNS Project is a open and volunteering project. We encourage self-sponsored participants to join this project with your servers, resolvers and insight to any technical discussion.
- Yeti DNS Project provides an open forum for the exchange and analysis of DNS related research. Work both inside and outside Yeti is welcome, but those based on implementation experience is given preference.
- Yeti DNS Project uses an [open mailing list](#) as the main collaboration tool, and will hold regular at lease two f2f meetings per year.

# Plan

- Yeti phase-2 Decentralized Domain Name System
  - 2020.3-2020.6 Request for comments
  - 2020.6-2020 .12 Prototype development, test in lab technical specifications update
  - 2021.1-2021.12 Run on test bed
- others

Thanks for listening!