# Single point of peering?
# Rischi nascosti negli exchange

**Antonio Prado**
*The Internet Floopaloo*



Meeting VSIX 2025

Padova, 26 novembre

# Intro

nodi sistemici di Internet

*single point of peering?*

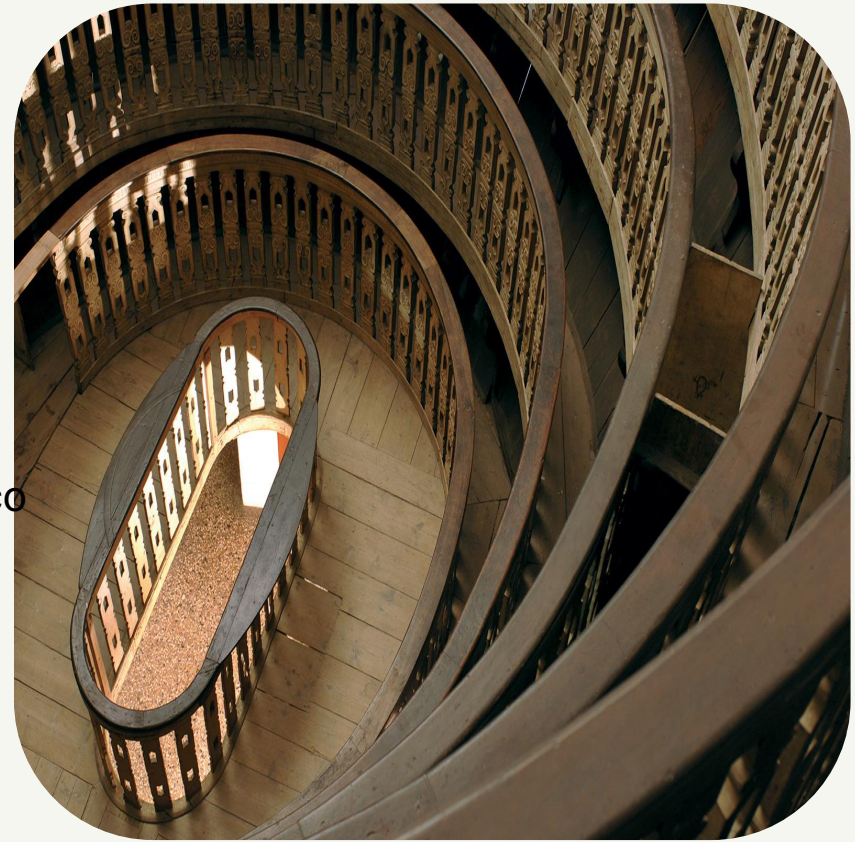
resilienza nazionale

NIS2 e CER

**policy**

# Il problema

# L’illusione della ridondanza



- Un operatore si percepisce ridondato quando ha 2 transiti, qualche PNI, 1 o 2 IXP, due router core ecc.
- Magari a guardare bene gran parte del traffico critico passa da **uno stesso exchange**, spesso in **un solo data center** e su **un solo fabric o route server**.
- Questo nodo diventa un **single point of peering**: se si ferma, si degrada o si rompe la connettività di interi ecosistemi.
- Il rischio è subdolo: non è scritto nelle architetture ufficiali, ma emerge da **come** usiamo gli IXP

# Che cos'è un *single point of peering*?

Non è un termine standard, ma una **situazione ricorrente**:
un solo nodo o fabric da cui dipende la maggior parte del nostro peering.
Può essere:

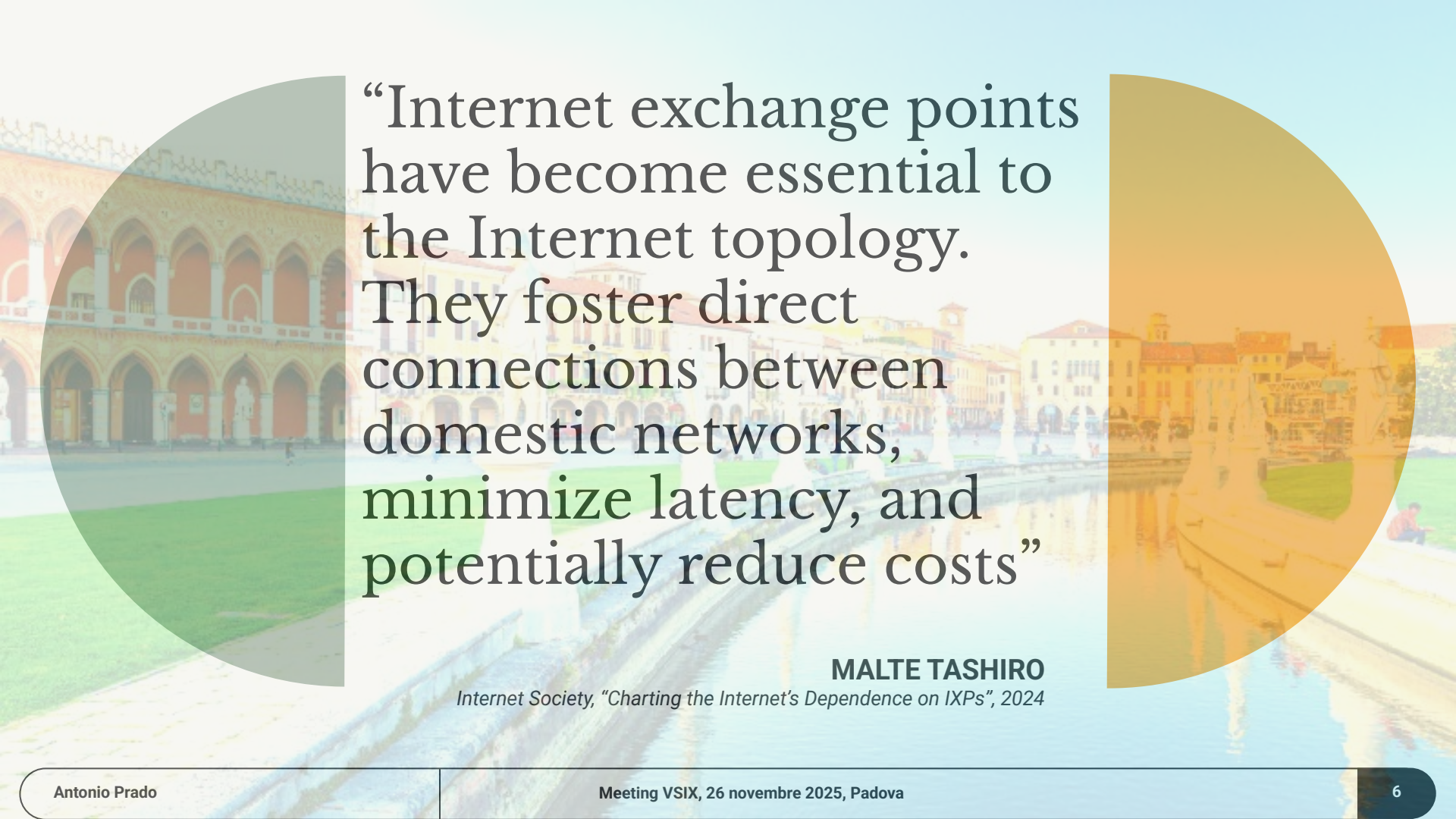
- un **singolo IXP** (o un solo PoP dell'IXP)
- un **route server** o una coppia di router al centro del peering
- una **tratta L2** verso un IXP remoto su cui viaggiano tutti i peer.

# Che cos'è un *single point of peering*?

Lo riconosco quando:

- **x% del traffico critico** (CDN, cloud, PA, DNS…) passa sempre da lì
- non esiste un **percorso alternativo equivalente** (in costo, capacità, latenza).

È quindi un **single point of failure travestito da interconnessione "redundant friendly"**.



“Internet exchange points have become essential to the Internet topology. They foster direct connections between domestic networks, minimize latency, and potentially reduce costs”

**MALTE TASHIRO**

*Internet Society, “Charting the Internet’s Dependence on IXPs”, 2024*

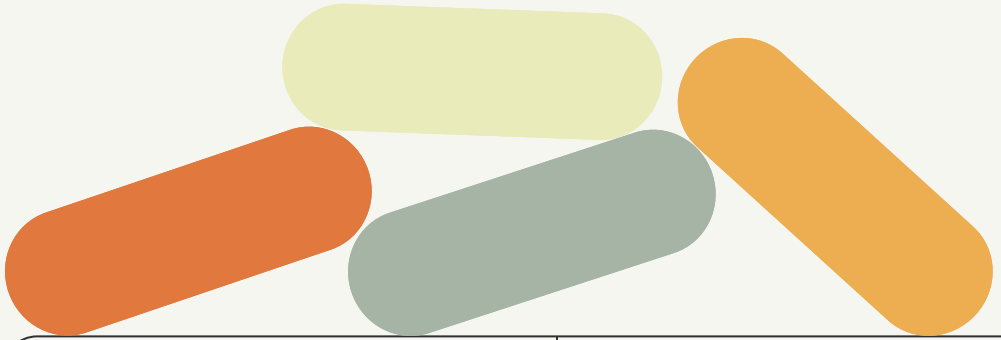
“I punti di interscambio Internet sono diventati elementi essenziali della topologia di Internet. Favoriscono connessioni dirette tra le reti nazionali, riducono al minimo la latenza e possono contribuire ad abbassare i costi.”

**MALTE TASHIRO**

*Internet Society, “Charting the Internet’s Dependence on IXPs”, 2024*

# Gli IXP non sono solo

*switch di peering*



Un IXP collega **centinaia di AS**: ISP, CDN, cloud, PA, ecc. Si concentrano spesso:

- **traffico domestico**
- **traffico internazionale**
- **servizi ausiliari**

Questo lo rende un **nodo sistemico**:

- influenza prestazioni e costi di un intero ecosistema
- può funzionare da **ammortizzatore** in caso di crisi
- oppure da **amplificatore** se diventa single point of peering.

Capire *come* usiamo gli IXP significa capire **dove è fragile** la nostra interconnessione.

# Tre modi in cui un IXP diventa

*single point of peering*

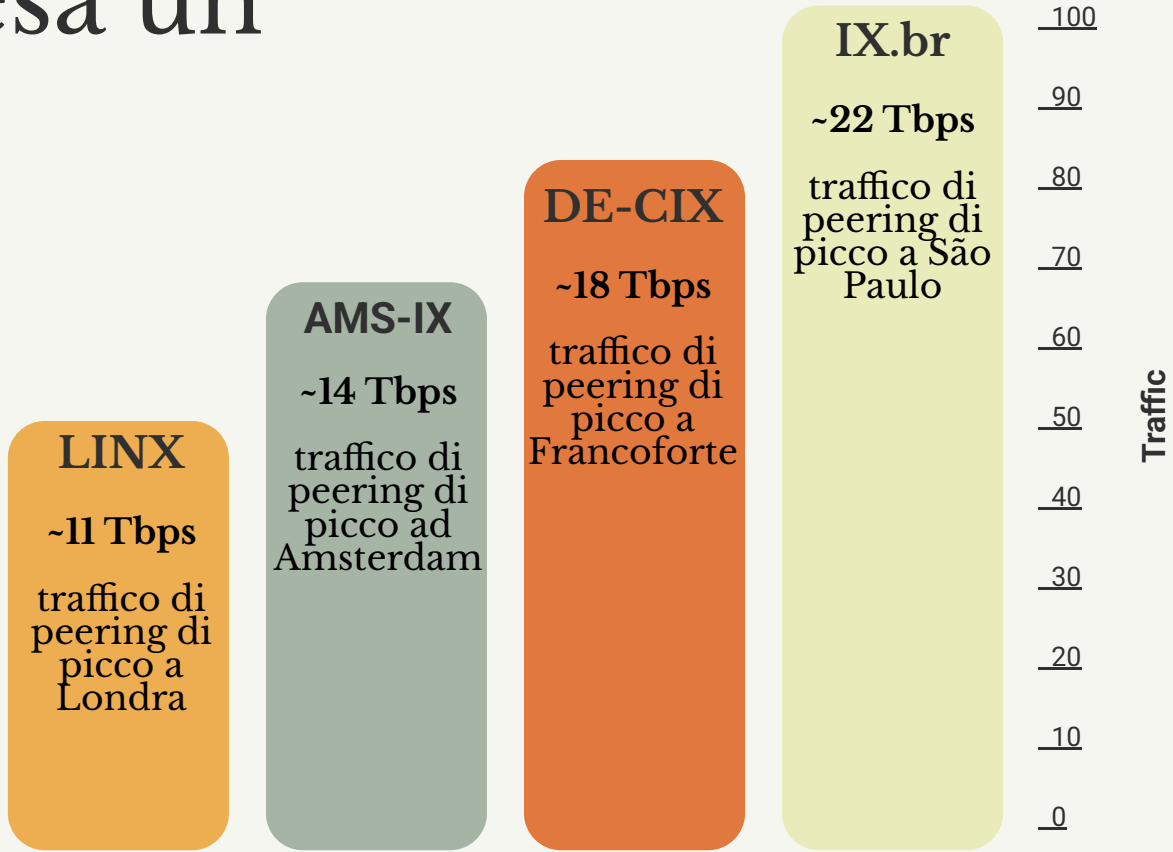
1. **Dipendenza topologica**
   Un solo exchange o un solo PoP concentra la maggior parte delle **sessioni BGP** e del traffico critico
2. **Dipendenza funzionale**
   Sullo stesso IXP si accumulano **route server**, DNS, CDN, servizi di sicurezza (blackholing, scrubbing…): un guasto colpisce **più funzioni contemporaneamente**
3. **Dipendenza organizzativo-economica**
   Nessuna alternativa realistica in termini di **costo, capacità, latenza**: anche se esistono altri IXP o transiti, di fatto **non li usiamo**

Risultato: l'IXP smette di essere "uno dei tanti punti di interconnessione" e diventa **il** punto da cui dipende l'intero ecosistema locale.

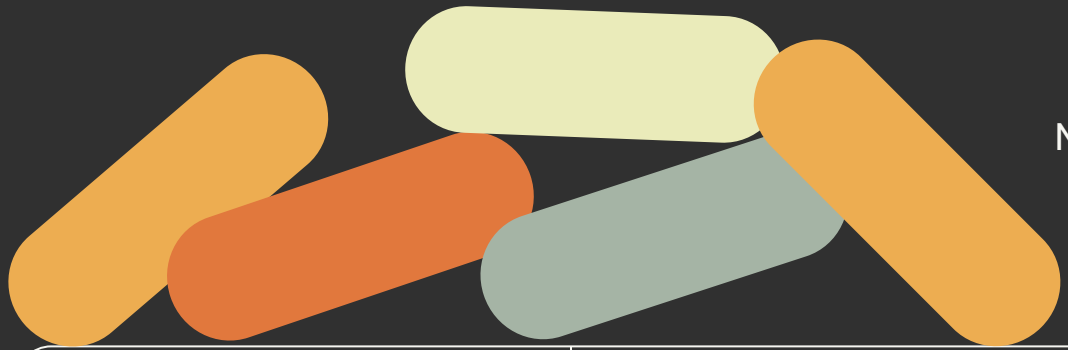
# Ma quanto pesa un grande IXP?

$$\sum$$

~65 Tbps



# Cosa succede quando un grande IXP ha un fault?



In alcuni outage reali su grandi IXP (AMS-IX, LINX LON1…):

- **oltre il 70-80%** dei percorsi che prima passavano dall'IXP smette di attraversarlo durante il picco dell'incidente
- fino a **circa 1/3 dei traceroute** perde del tutto la connettività verso la destinazione per alcuni minuti.

Molto traffico viene riprotetto via **transito IP**:

- latenza media che può crescere anche di **oltre il 50%** nel caso peggiore
- percorsi più lunghi, spesso meno prevedibili.

Non si rompe l'Internet, ma per gli utenti coinvolti:

- **servizi irraggiungibili**
- degrado forte di qualità
- e costi imprevisti lato operatori.

*case study*

# Un grande IXP ha starnutito!

**QUANDO e DOVE**

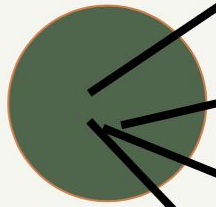
2021

LINX LON1, uno dei principali exchange di Londra

**COSA**

Problema di configurazione e infrastruttura sul fabric principale

**EFFETTI**



- oltre **l'80%** dei percorsi che prima passavano da LINX smette di attraversarlo durante il picco dell'incidente
- fino a **~1/3 delle destinazioni** diventa temporaneamente irraggiungibile
- sul piano BGP, **>200%** di incremento degli annunci di routing (instabilità diffusa attorno all'IXP)
- circa il **90% dei membri** risulta in qualche misura impattato

# Da un singolo fault a un rischio sistemico

Un incidente su un grande IXP **non** è solo un guasto di rete:

- impatta **reti diverse**, con ruoli diversi
- colpisce **più servizi** contemporaneamente.

La severità non dipende solo dal fault, ma da **come siamo connessi**:

- chi usa l'IXP come *uno dei tanti* punti di scambio → degrado limitato
- chi lo usa come *single point of peering* → perdita di connettività o instabilità prolungata.

In alcuni Paesi, uno o due IXP di questo tipo coincidono di fatto con:

- la **"dorsale informale"** del traffico nazionale
- una parte significativa dei servizi digitali essenziali.

Qui il problema smette di essere solo tecnico:

diventa un tema di **resilienza nazionale, sicurezza e sovranità digitale.**

# Gli IXP nel quadro normativo italiano ed europeo

1. La Direttiva **NIS2** e il d.lgs. **138/2024** collocano gli IXP nel settore **“Infrastrutture digitali” ad alta criticità**

2. Gli IXP sono elencati nel settore 8 “Infrastrutture digitali”, insieme a DNS, TLD...

3. L’IXP di medie dimensioni è qualificato come “soggetto essenziale” NIS2, con obblighi per sicurezza e incidenti.

4. A livello UE, gli IXP rientrano tra i settori critici della Direttiva CER, ma sono regolate soprattutto da NIS2.

5. Alcuni IXP possono essere designati nel Perimetro cibernetico o in altre liste nazionali di soggetti critici; non è automatico.

6. Secondo le norme, un grande IXP è già oggi trattato come **infrastruttura digitale essenziale** per la continuità dei servizi.

## ESSENZIALE

Linguaggio NIS2

Garantisce il funzionamento quotidiano dei servizi digitali

Se si ferma, molte cose smettono semplicemente di funzionare

## CRITICO

Linguaggio CER

La sua interruzione genera disservizi gravi e immediati

È tra i primi elementi da proteggere in uno scenario di crisi

## SISTEMICO

Linguaggio Tecnico

Un guasto locale produce effetti a catena sull'ecosistema

È il punto in cui tutto si tiene insieme

## STRATEGICO

Linguaggio Politico/Industriale

Influenza nel tempo autonomia e competitività del Paese

Le scelte su di esso orientano il futuro della rete nazionale

# Come evitare il *single point of peering*

## Misurare la dipendenza

Stimare quanta parte del traffico critico (CDN, cloud, PA, DNS…) passa da **ciascun IXP / PoP / RS**

## Diversificare i punti di interconnessione

Più peer? Non basta: **più IXP indipendenti**, più PoP, più route server / sessioni bilanciate

## Prevedere veri percorsi alternativi

Transito, PNI e altri IXP che siano **realmente usabili** in caso di fault (capacità, policy, costi, latenza accettabile)

# Come evitare il *single point of peering*

## Verificare i piani di failover

Simulare l'assenza di un IXP / RS / tratta L2 e vedere **cosa succede davvero** (BGP, qualità esperienza utente, costi)

## Chiedere di più agli IXP

Trasparenza su architettura, resilienza, sicurezza BGP, gestione incidenti:
non solo "quanti peer ci sono", ma **quanto è robusto il nodo sistemico**

## Osservare e loggare gli incidenti

Raccogliere dati su fault e degradi legati agli IXP (latency, loss, route change) per **correggere la progettazione** invece di basarsi solo su sensazioni

# Se gli IXP sono essenziali, cosa deve cambiare nelle policy?

**Requisiti minimi chiari e proporzionati**

Sicurezza BGP, resilienza fisica e logica, trasparenza su architettura e incidenti, con oneri diversi per grandi e piccoli IXP

**Riconoscere gli IXP come infrastrutture digitali essenziali**

**Incentivare pluralismo di IXP e di siti (no a un solo grande IXP)**

**Decisioni su IXP prese con operatori, NOG, associazioni**

# Tre idee da portarsi a casa

Gli IXP sono nodi sistemici

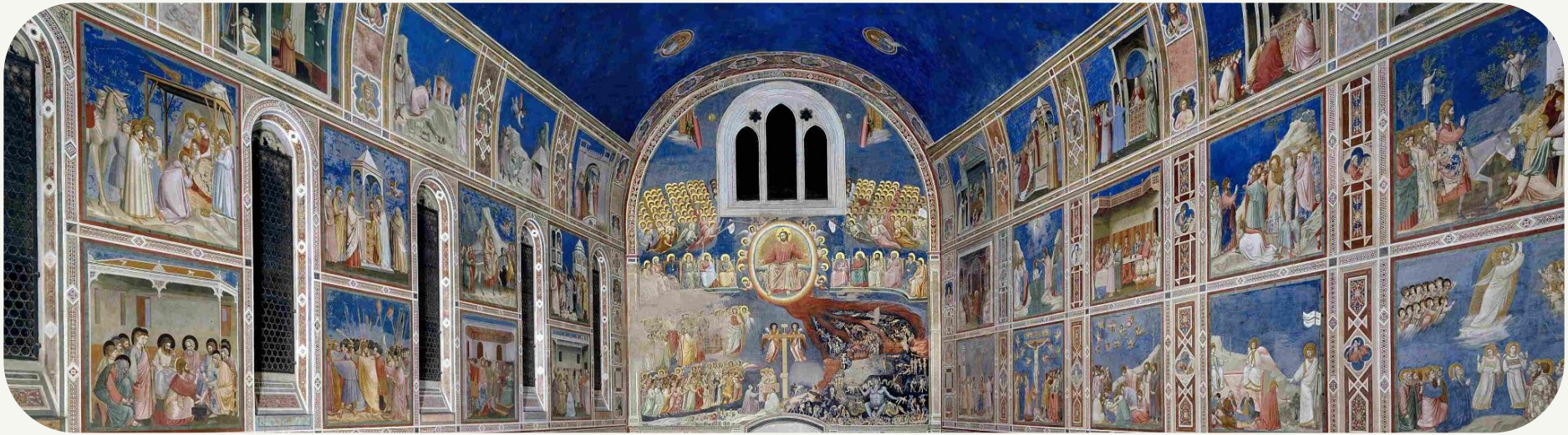
Il rischio è spesso nascosto

La soluzione è tecnica e politica insieme

da loro dipendono prestazioni, costi e continuità di molti servizi

*single point of peering* anche in reti che sembrano ridondate

Progettazione + requisiti minimi + pluralismo
=
ecosistemi meno fragili



# Single point of peering?
# Rischi nascosti negli exchange
# Domande?

**Antonio Prado**
*The Internet Floopaloo*



Meeting VSIX 2025

Padova, 26 novembre