Decentralised Data Delivery Markets (3DMs)

An Open Problem Statement and Call for Ideation

IRTF ICNRG

10th March 2021

Yiannis Psaras

Research Scientist, Protocol Labs

Problem

Place incentives for fair exchange and fast delivery on top of permissionless P2P networks.

in other words:

Build a **decentralised CDN** based on a P2P network.

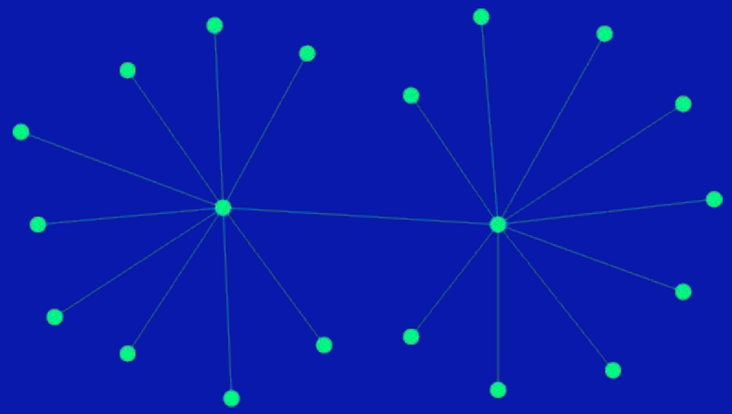
Incentives are tricky to get right.

Network connectivity and formation is central.

Achieving fair exchange without a trusted third party in real time is key to success.

Setting the scene

Players in 3DMs



Cold Storage Providers: can provide access to content, but

1. access is slow (will first have to decrypt) and
2. content lives in one (or very few) places only

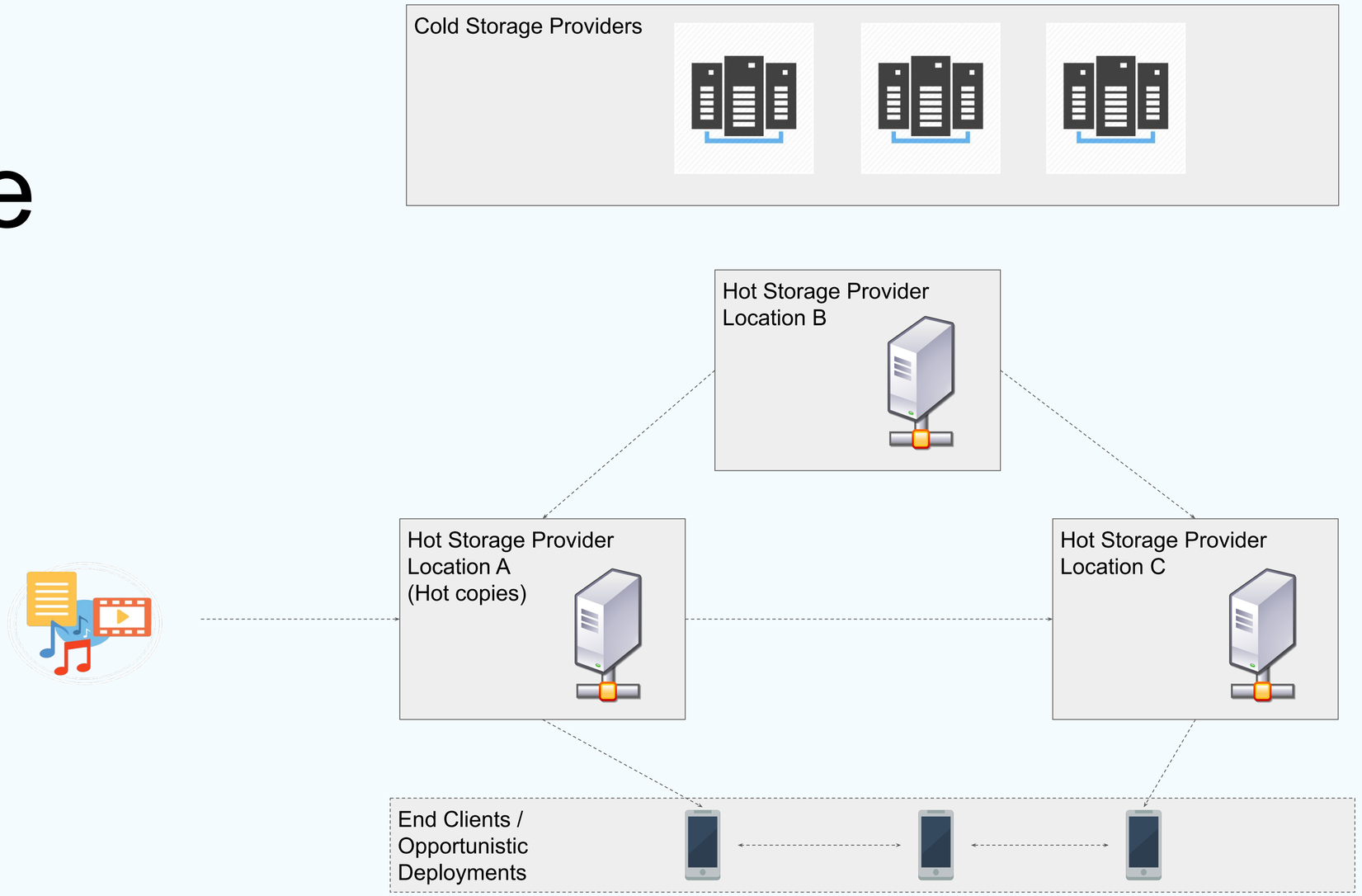
Hot Storage and Delivery Providers

- here’s where all the magic happens
- content discovery and content routing system
- content placement
- content copy selection

Clients: want fast access to content

Publishers: want a hot copy available closeby

3DM Architecture



Self-certified, named, or content-addressed data is key to achieve the level of decentralisation desired here.

Focus

Three Problem Areas

- Data Delivery Metering & Fair Exchange
- Distribution Graph Forming
- Economic Model

Metering and Fair Exchange

- Metering
- Graph Forming
- Economics

Problem Definition:

Desired Properties

➔ ***The exchanges of value MUST be verifiable and correct***

- ***Fairness:***
  - The payment MUST only happen if the delivery happens
  - The SLA for bandwidth/latency SHOULD match what has been agreed
- ***Verifiability***:
  - Both parties MUST be capable of verifying that the exchange was performed correctly
  - *Bonus property*: Anyone SHOULD be able to verify that the exchange was performed correctly

Challenges & Requirements

Ensure Fairness

- How to verify that the file being transfer is the one requested?
- How to verify that the client has received the file?

- How to avoid a malicious actor causing un-rewarded work, hence wasting the others resources?

- On the impossibility of fair exchange without a trusted third party. Technical report. Henning Pagnia and Felix C. Gärtner. 1999
  - How to avoid collusion when adding a third-party (e.g. Referee)?
  - New developments made it possible to have an impartial third party (e.g. smart contract) or rely on third party just for disputes

Challenges & Requirements

Experience

- How to make the transfers start instantaneously?
- How to support third parties paying for the usage/content?
- How to make it private (e.g. that others don’t know who is requesting what)?

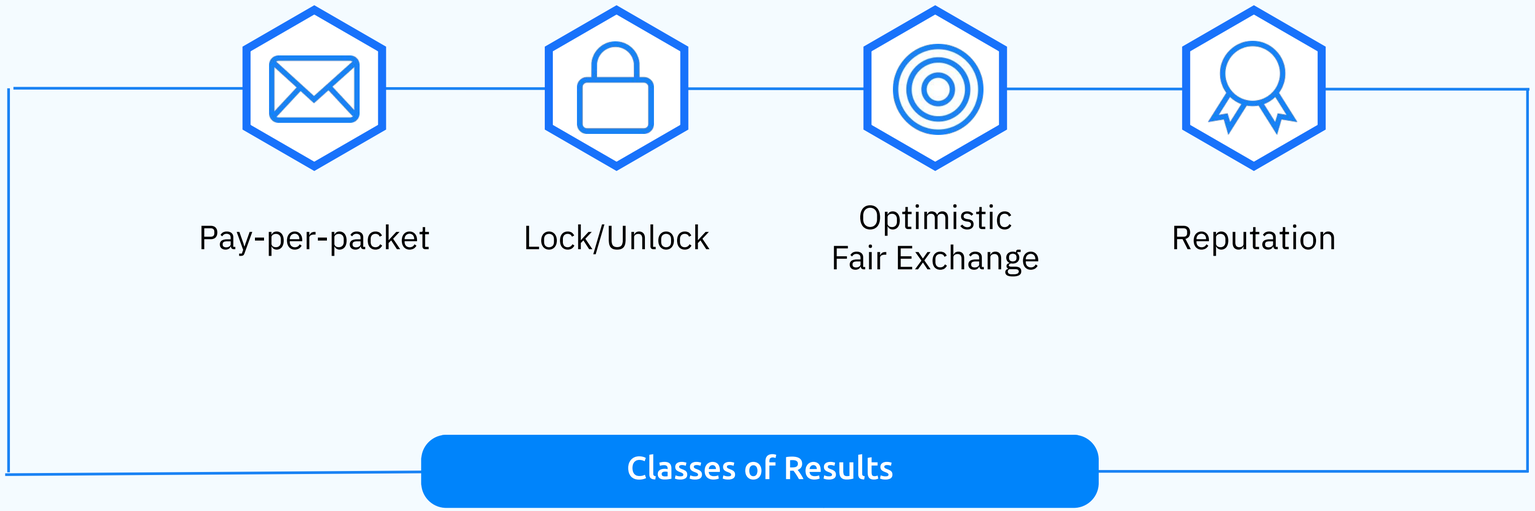
Challenges & Requirements

Performance

- How to overcome the send-and-halt pattern in order to max bandwidth throughput
  - Send-and-halt is typical of the pay-per-packet solutions in which the next packet is only sent when the previous was paid for
- How to support multipath (i.e. fetching from multiple sources)

Literature Review

- State of the art solutions do not fit as they need a central point of control for metering and mediating the exchange



Distribution Graph Forming

- Metering
- Graph Forming
- Economics

Problem

How can we construct an efficient, distributed CDN on top of cold storage providers to enable access to content, discovery and delivery?

How is the network formed, and how is data ingested into the CDN cache?

How do we efficiently route requests for data, and the data itself?

How do we account for the economics required to incentivize this?

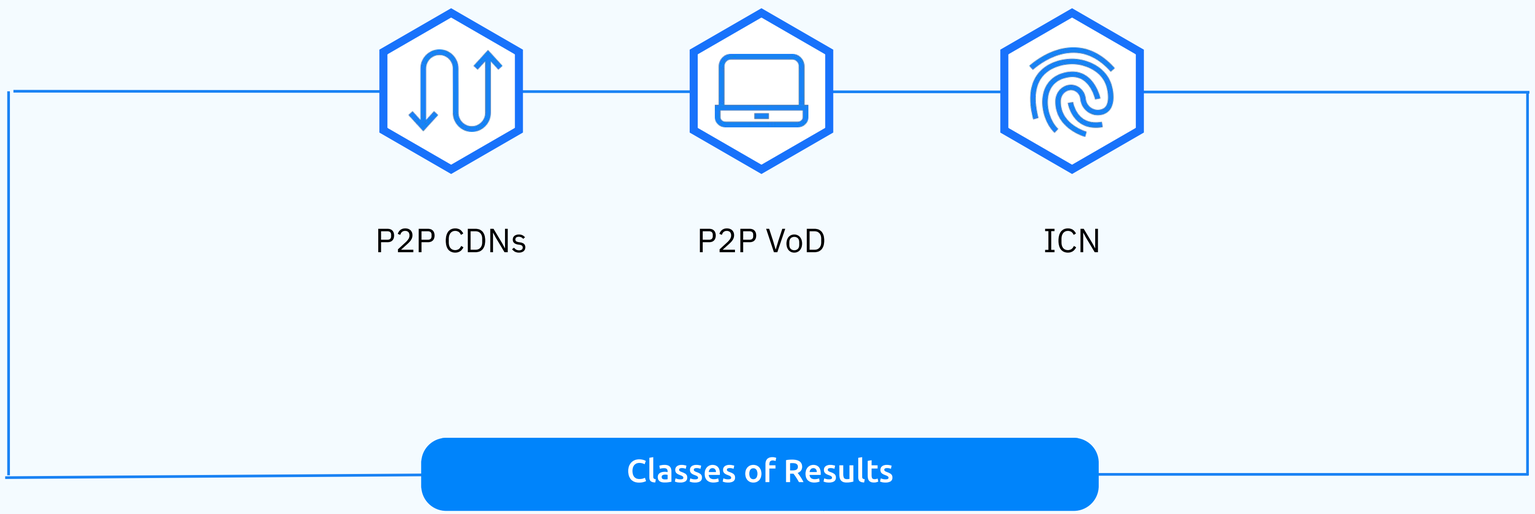
Problem Definition:

Desired Properties

- ➔ *The system MUST always be **able to discover** content and satisfy content requests*
- ➔ *The system MUST **replicate content to different storage points** in order to reduce delivery times and maximize performance.*
- ➔ *Providers MUST **follow the economic model** and the system MUST make sure that **Providers do not misbehave**.*
- ➔ *The system MUST be **permissionless***
  - ◆ *Anyone should be free to join and set up a Provider node to contribute to the network.*

Literature Review

- State of the art solutions do not fit as they need a central point of control for metering and mediating the exchange



DHT/PubSub

Name-based Routing

DNS-like system

e.g., CF’s ENS Gateway

Challenges

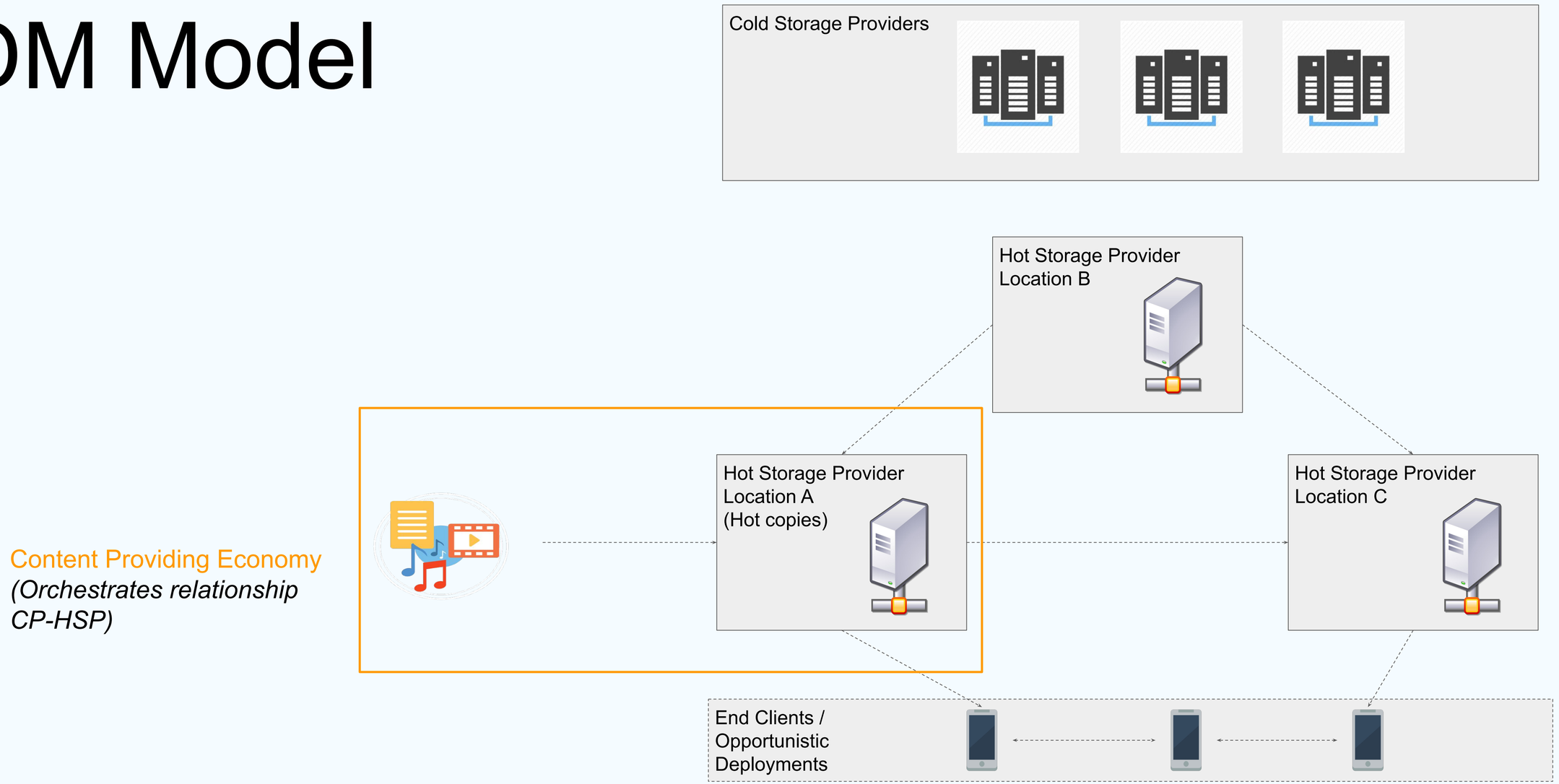
Challenges with Name-based Routing

- **New design** introducing higher risk
- Needs to be tightly coupled to the **economic model**
  - How can we augment naming schemes to account for economic transactions?
- **Bootstrapping** the network and filling in **routing tables**
- Pending Interest Tables (PIT) may not be needed, could introduce attack vectors
- **Tradeoffs** in symmetric vs asymmetric routing
  - Symmetric routing **increases traffic** (multi-hop transfer) and some centralization of failure
  - Symmetric routing also gains huge **caching benefits** on subsequent requests
  - There is a tipping point in the request pattern (i.e. popularity) after which switching to name-based routing is more efficient.

Economic Model

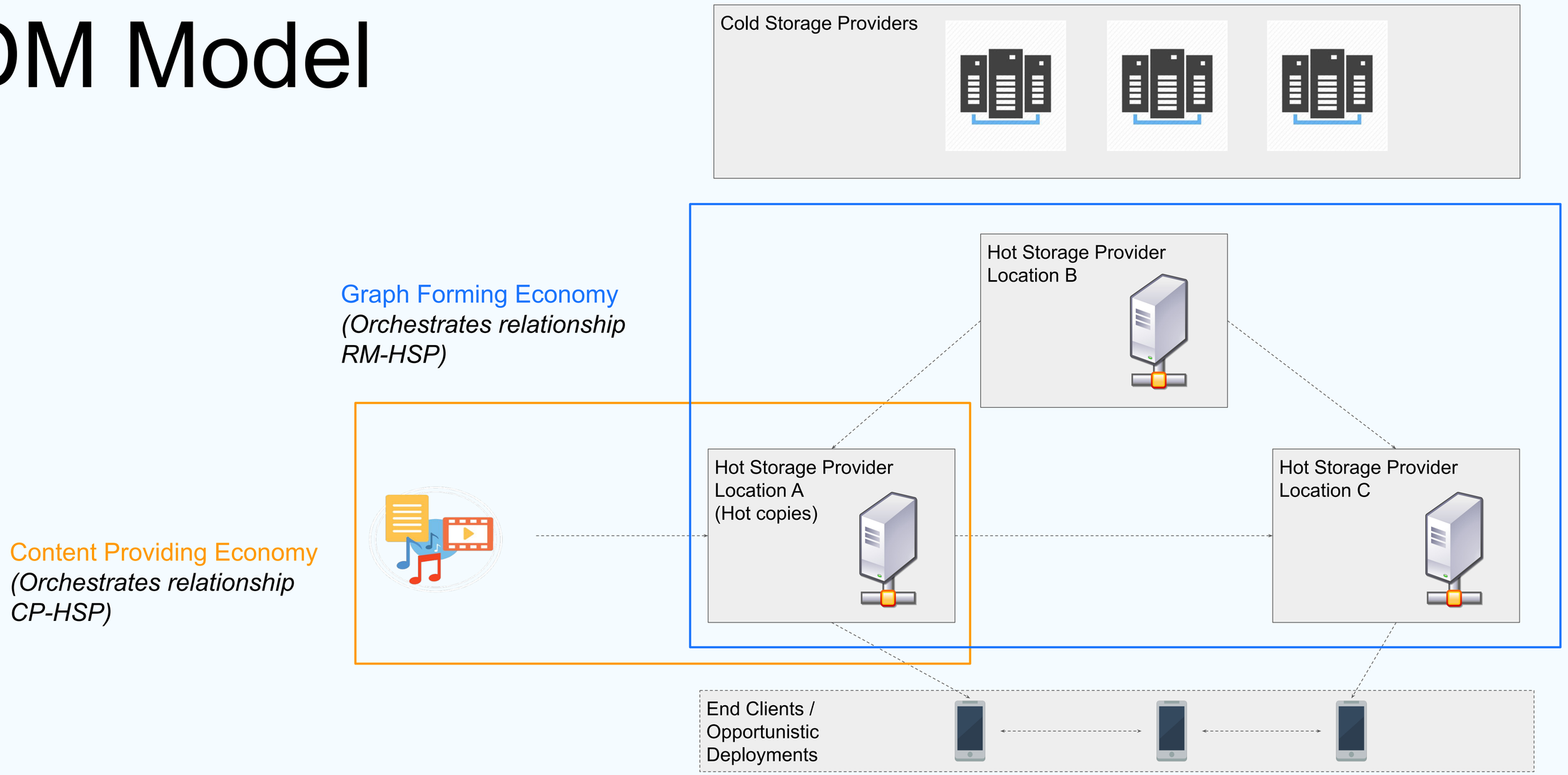
- Metering
- Graph Forming
- Economics

3DM Model

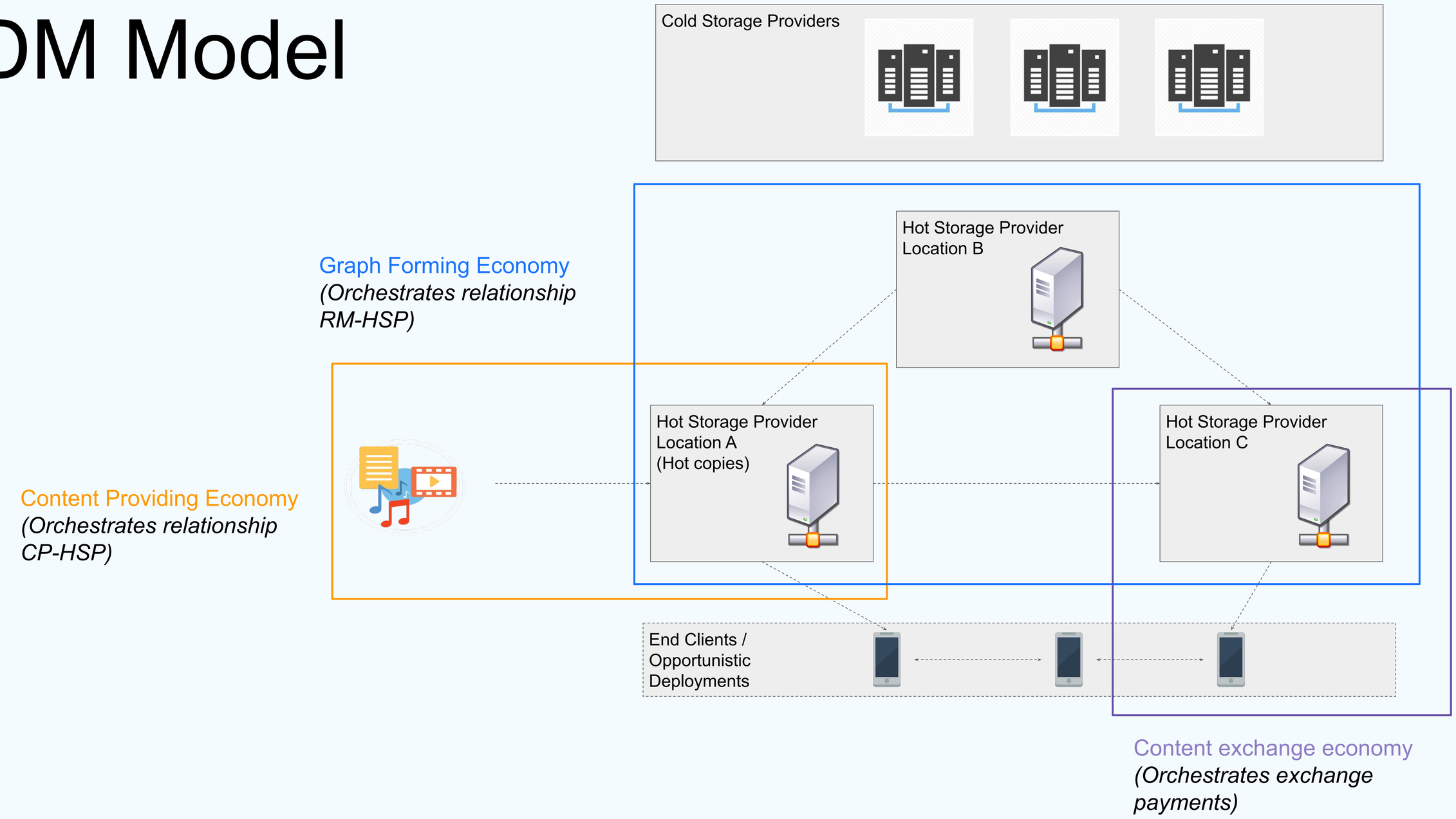


Content Providing Economy
(Orchestrates relationship CP-HSP)

3DM Model


Cold Storage Providers
Graph Forming Economy
(Orchestrates relationship RM-HSP)
Hot Storage Provider Location B
Content Providing Economy
(Orchestrates relationship CP-HSP)
Hot Storage Provider Location A (Hot copies)
Hot Storage Provider Location C
End Clients / Opportunistic Deployments

3DM Model


Cold Storage Providers
Graph Forming Economy
(Orchestrates relationship RM-HSP)
Hot Storage Provider Location B
Hot Storage Provider Location A (Hot copies)
Hot Storage Provider Location C
Content Providing Economy
(Orchestrates relationship CP-HSP)
End Clients / Opportunistic Deployments
Content exchange economy
(Orchestrates exchange payments)

Ideas from Papers 📰

- ***Edge-MAP: Auction Markets for Edge Resource Provisioning***
  - *Use of individual local markets/auctions at the base-station of each cell.*
  - *Bidders adjust their demand according to their local view.*

- ***How Neutral is a CDN?***
  - *Profit maximizing CDNs maximise fairness.*

- ***“An economic mechanism …” paper series***
  - *Economics of hybrid-CDN request routing and replica placement.*

- ***A Market Protocol for Decentralized Task Allocation***
  - *Use of reserve price to drive the auction and reach equilibrium.*

- ***Proof-of-prestige: A Useful Work Reward System For Unverifiable Tasks***
  - *Use of a volatile token minted as a budget throughout time can be transferred for useful work.*
  - *No intrinsic value*

- ***Skrivener: Providing Incentives in Cooperative Content Distribution***
  - *Credit and confidence to decide on relationship with entities.*

- ***Collusion-resilient Credit-based Reputations for Peer-to-peer Content Distribution***
  - *Use credit-diversity to avoid collusion*

Ideas from Papers 📰

Content Providing Economy

- ***Edge-MAP: Auction Markets for Edge Resource Provisioning***
  - *Use of individual local markets/auctions at the base-station of each cell.*
  - *Bidders adjust their demand according to their local view.*

Graph Forming Economy

- ***How Neutral is a CDN?***
  - *Profit maximizing CDNs maximise fairness.*
- ***“An economic mechanism …” paper series***
  - *Economics of hybrid-CDN request routing and replica placement.*
- ***A Market Protocol for Decentralized Task Allocation***
  - *Use of reserve price to drive the auction and reach equilibrium.*

Content exchange economy

- ***Proof-of-prestige: A Useful Work Reward System For Unverifiable Tasks***
  - *Use of a volatile token minted as a budget throughout time can be transferred for useful work.*
  - *No intrinsic value*
- ***Skrivener: Providing Incentives in Cooperative Content Distribution***
  - *Credit and confidence to decide on relationship with entities.*
- ***Collusion-resilient Credit-based Reputations for Peer-to-peer Content Distribution***
  - *Use credit-diversity to avoid collusion*

Challenges

Challenges with the Economic model

- **Sybil Attacks:** Create sybils and forge client requests and waste Hot Storage Providers' resources
- Colluding Attacks: force artificial money transfers (and revenue) between colluding parties.
- **Data Ransoming:** Deliver and get paid for all but the last few bytes of a file.
- Pending Interest Tables (PIT) may not be needed, could introduce attack vectors
- What **metadata** should be included in the name, as semantics to drive economic relationships and data exchange?
- How can authenticated and/or self-certified data help avoid some of these attacks

Thank you

Get involved:
https://github.com/protocol/resnetlab

Get in touch: yiannis@protocol.ai