wuala

by LACIE

Wuala: Distributed Storage System

NASA Goddard Space Flight Center
2009-11-09
Dominik Grolimund (dominik@wuala.com)

Overview

Summary

Wuala is an online storage, based on a novel grid technology

Started research and development at ETH Zurich in 2004/2005

Founded in 2007 by Dominik Grolimund and Luzius Meisser

12 people today, mainly engineers, expanding

Launched in 2008, now hundreds of thousands of users and millions of files

Sold the company to LaCie in 2009

Self-financed until acquisition

Wuala now an autonomous subsidiary of LaCie

Team

Team of 12 people, mainly software engineers

9 have a M.Sc./Ph.D. in computer science from ETH Zurich/EPF Lausanne

Expanding

Dominik Grolimund, co-founder and CEO

Master's degree in computer science ETH Zurich

Unitech Exchange programme, business and management

Founded Caleido in 1998, sold more than 35'000 licenses of a CRM software

Luzius Meisser, co-founder and CTO

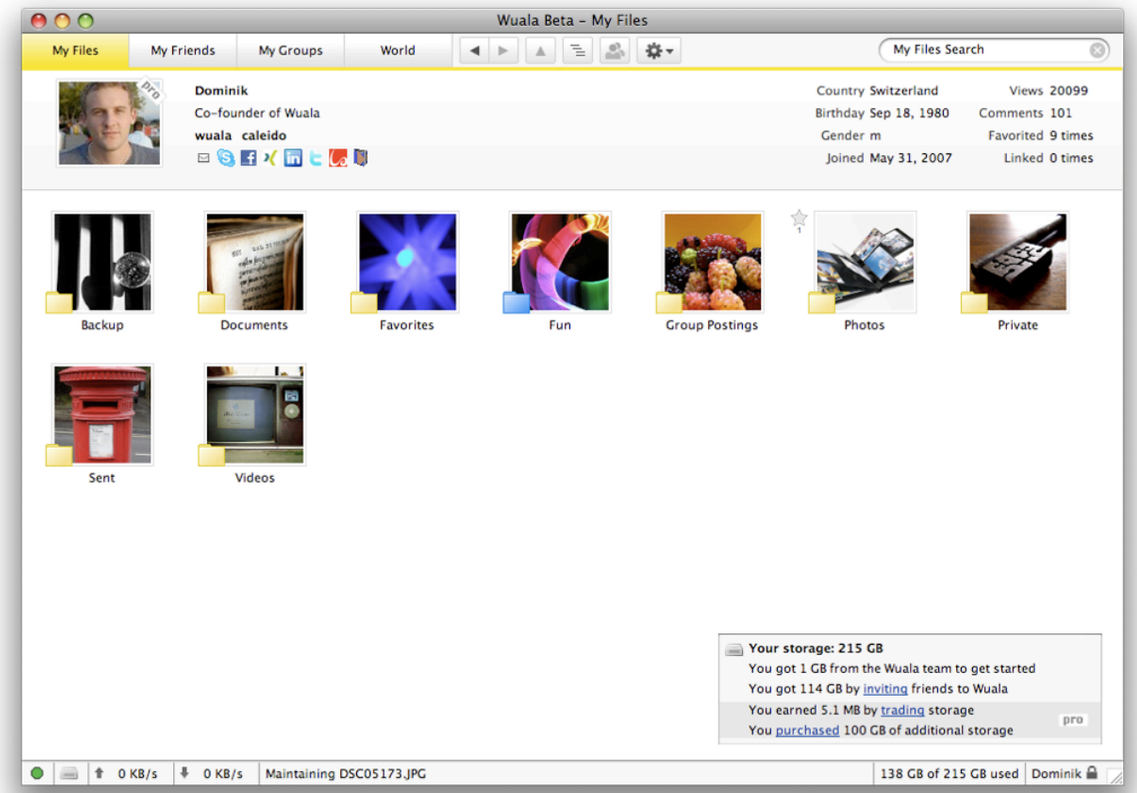
Master's degree in computer science ETH Zurich

Unitech Exchange programme, business and management

Product

Wuala is an online storage

- Backup
- Store files securely in the cloud
- Access from anywhere
- Share with friends and groups



Customers:

- Private users
- Universities (Wuala Campus)
- Small companies
- Digital content creators

Technology

Wuala is based on a novel technology that reduces our costs

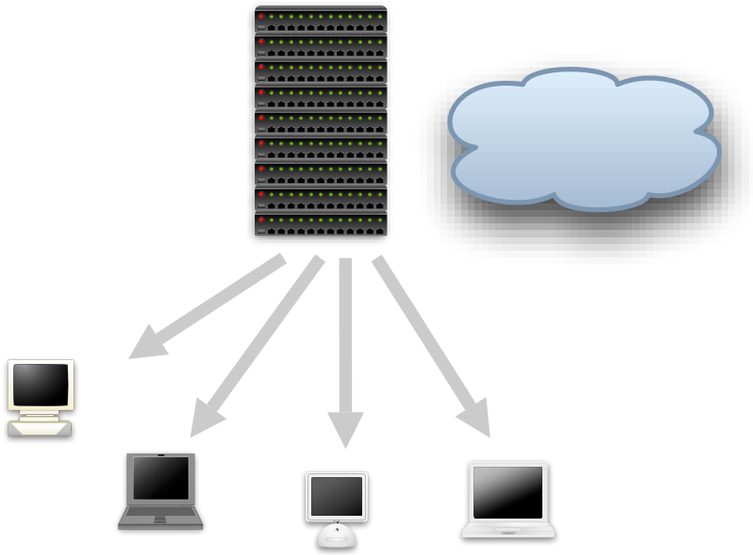
We harness idle resources of participating computers (P2P/grid)

Dominik and Luzius started at ETH with semester/lab/Master thesis

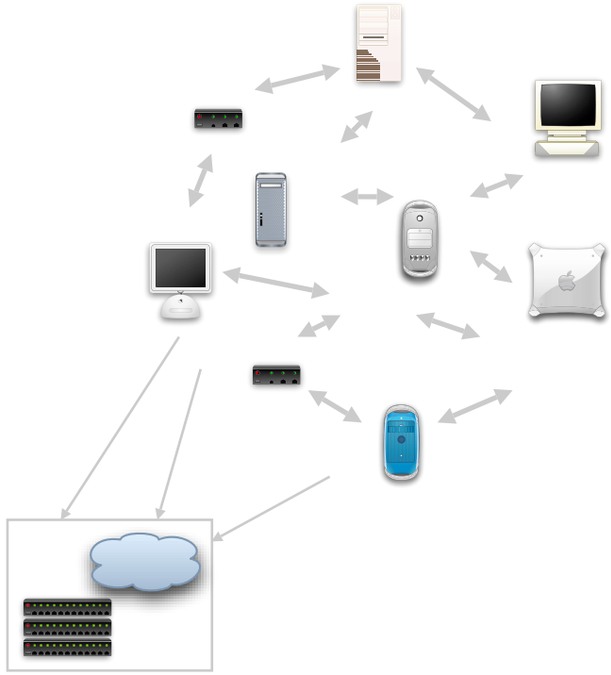
Afterwards, 25 students did their thesis on Wuala

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Traditional



Our solution



Awards

wuala by LACIE

lift CONFERENCE

Le Web 3 '07 FOURTH EDITION

Webware 100 2008

venturelab FAST TRACK FOR START-UPS

Plugg

CTI START-UP

RED HERRING 100 EUROPE FINALIST

ReadWriteWeb Best Products 2008

swiss made software

RED HERRING GLOBAL FINALIST 200

RED HERRING EUROPE WINNER 100

PC Pr@xis 11/2008 Preis/Leistung sehr gut Qualität gut

DIE 200 BESTEN WEBSITES 2009

International Press Coverage

wuala by LACIE

PC MAGAZINE

downloadsquad

Tages-Anzeiger

SonntagsZeitung

TechCrunch

www.cashdaily.ch

INNOVATION

Der erste sichere Online-Speicher

heise online

utzen: den weltweit einzigartigen
ETH-Spin-off in vierjähriger Arbeit.

WUALA EIN MULTIFUNKTIONALER ONLINE-SPEICHER

Technology Monitor

Online storage

Thanks for the men

Sep 10th 2008

From Economist.com

A mathematical trick may allow people to scatter their computer files across the world's hard disks

Wuala

IF YOU have lots of unused storage space on your hard disk, then why

Scatter brains

indeed, even if your computer is switched off. That desideratum is what a Zurich-based firm called Caleido is aiming to provide, with a free online storage service known as Wuala that was recently introduced to the public.

Though the idea underlying it is simple, Wuala requires some nifty technology to make its distributed system work reliably. In particular, its developers, Dominik Grolim

SPIEGEL ONLINE

CHIP ONLINE de

Mashable SOCIAL NETWORKING NEWS

Festplatte mit sozialer Ader

set. Dank schnellen und nahezu überall verfügbaren Internet-Verbindungen boomen Dienste, welche Datenspeicher auf einem Internetserver an-

ter Daten anfallen. Die Anwender ihrerseits erhalten kostenlos Online-Speicher im Verhältnis zum Platz, den sie auf ihrer Festplatte für das

Economist.com

ウィキペディア
フリー百科事典

本文

Wuala

出典: フリー

Wualaは、スイス連邦のCaleido AG社のファイル共有ソフトである。

目次 [非表示]

1 概要
2 特徴
3 ストレージ容量
4 セキュリティ

ナビゲーション

- メインページ
- コミュニティ・ポータル
- 最近の出来事
- 最近更新したページ
- ヘルプ
- 井戸端
- お知らせ
- バグの報告
- 寄付

検索

特徴

今までの多くのファイルスト
サービスであったが、Wualaで
簡単にできるようになってい

ars technica
the art of technology

TechCrunch

Previous Post

Next Post

Wuala Launches Social Grid Storage In Public Beta Tomorrow

by Mike Butcher on August 13, 2008

37 Comments

This has to be some kind of record – a startup launching a public beta on the day it said it would. Wuala, the P2P 'social grid storage' startup from Switzerland, launches its public beta tomorrow at www.wuala.la. Users will be able to simply click on a button on the site to start the service (it's a Java app). That's it. You can drag-and-drop stuff into it for file backup, photo and video sharing, or making files available publicly.

Here's a more detailed description, from our post

The underlying core tech behind Wuala is base
Swiss Federal Institute of Technology). The file
across the "Wuala Grid" of users, and mirrored on Wuala's servers – so you don't have to rely
sers start with 1 GB of storage but can get
pace or by buying additional storage. You
want more, you can make more space
embers. But users don't have to trade
100 Euros. All files are encrypted on the
cess to which folder. No one else –

wuala

en Datenspeicher
H-Absolventen für
Aufsehen. Mit opti-
nce und maximaler
eien im Internet
stauschen oder
- eine neuartige
möglich machen.

Gründung
Frühling 2007

Standort
Zürich

Branche
Speichersoftw

Internetadr
http://wua.la

Datenfluss und hoher Download-Geschwindigkeit.

Nicht mehr Speicher, sondern bessere Qualität

Slashdot

ZDNet

GIGAOM

ReadWriteWeb

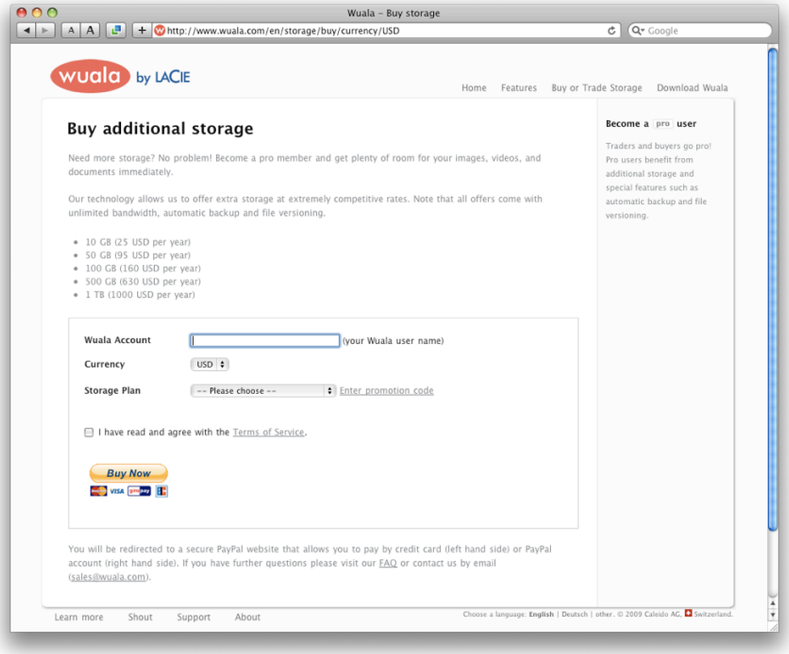
Webware

NZZ

Business Model

- “Freemium”: 1GB for free, pay for more (or trade)
- Premium offerings (backup, file versioning, etc.)
- Wuala Campus: special offering, now launched with ETH

- Soon: Revenues through DAS and NAS sales via LaCie



Wuala on NAS

wuala by LACIE

Trade storage on NAS for Wuala storage

Backup NAS to Cloud

Product

Store Files Online

wuala by LACIE

Wuala Beta – My Files

My Files | My Friends | My Groups | World | My Files Search

Dominik
Co-founder of Wuala
wuala caleido

Country Switzerland
Birthday Sep 18, 1980
Gender m
Joined May 31, 2007

Views 20099
Comments 101
Favorited 9 times
Linked 0 times

Backup | Documents | Favorites | Fun | Group Postings | Photos | Private

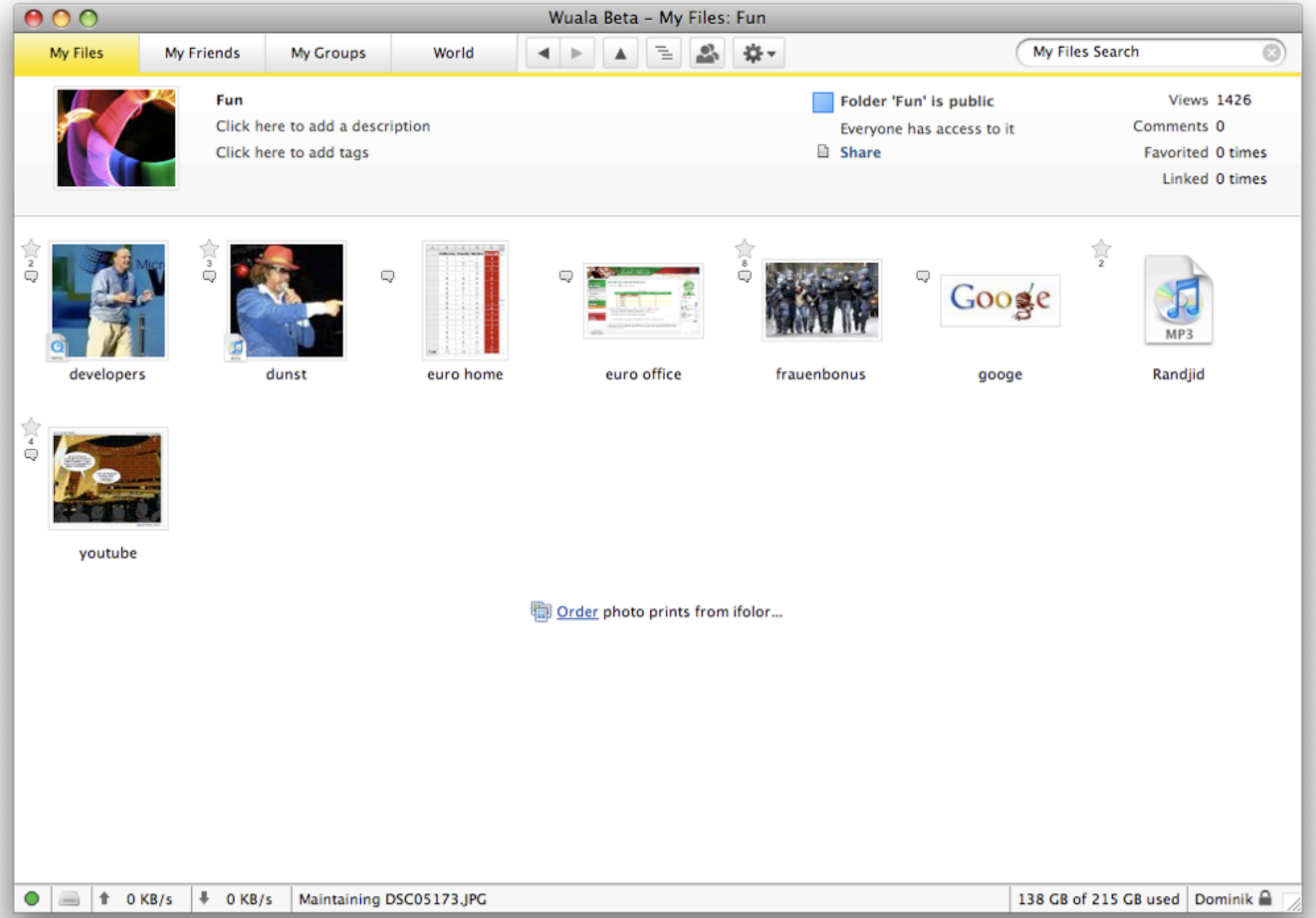
Sent | Videos

Your storage: 215 GB
You got 1 GB from the Wuala team to get started
You got 114 GB by inviting friends to Wuala
You earned 5.1 MB by trading storage
You purchased 100 GB of additional storage
pro

0 KB/s | 0 KB/s | Maintaining DSC05173.JPG | 138 GB of 215 GB used | Dominik

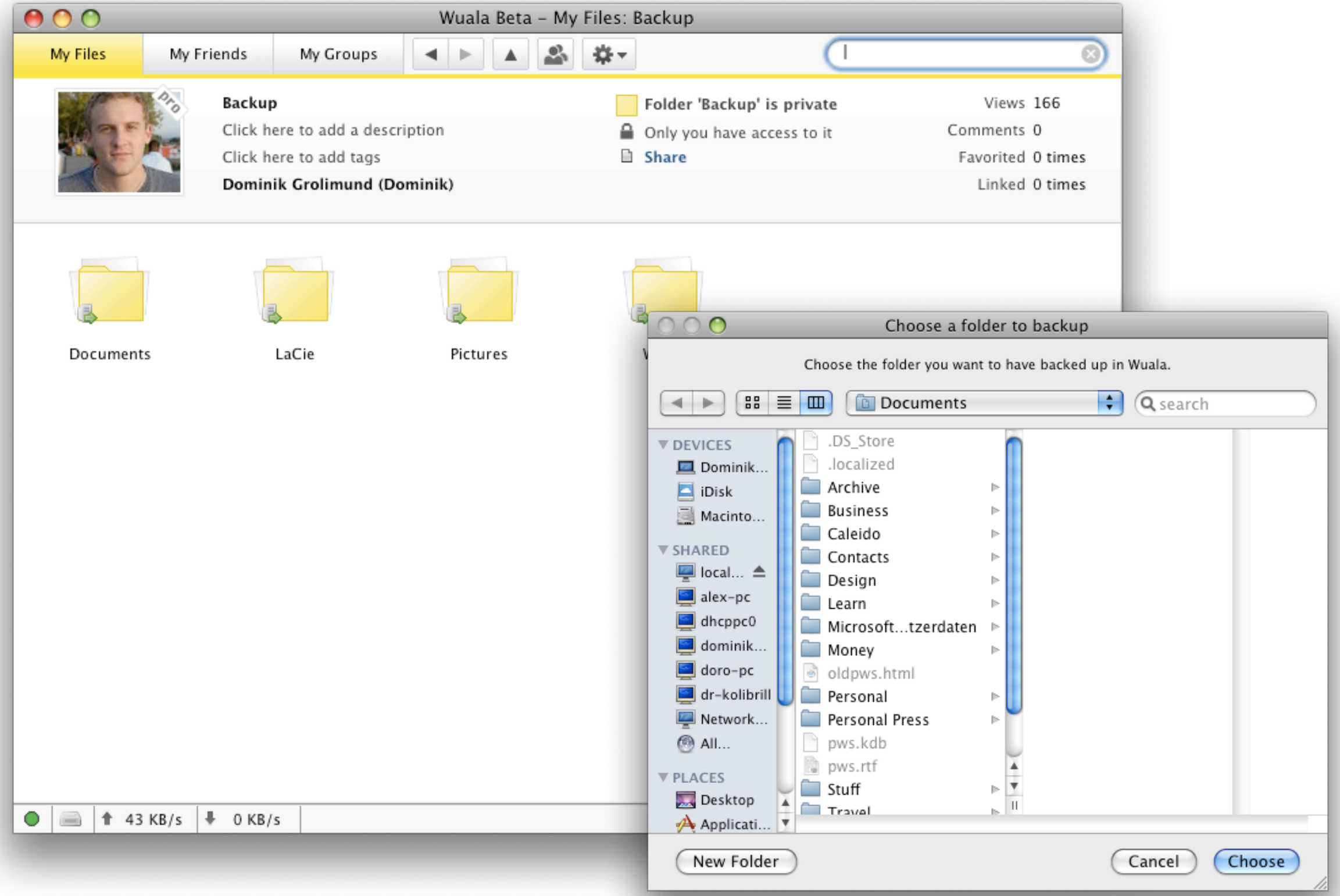
Any File, Any Size

wuala by LACIE



Backup: PC to Cloud

wuala by LACIE



Share

wuala by LACIE

Wuala Beta – My Files: 2007-07 Schweizer Ferien

My Files | My Friends | My Groups | World | My Files Search

2007-07 Schweizer Ferien
Click here to add a description
ch schweiz hiking mountains

Folder '2007-07 Schweiz...' is public
Everyone has access to it
Share

Views 1288
Comments 0
Favorited 0 times
Linked 2 times

DSC 1248 | DSC 1291 | DSC 1292
DSC 1366 | DSC 1372 | DSC 1377
DSC 1509 | DSC 1512 | DSC 1530

51 KB/s | 0 KB/s | Maintaining DSC05197.JPG | 138 GB of 215 GB used | Dominik

Share

Visibility
Email
Link
Badge
Bookmark

Folder '2007-07 Schweizer Ferien'
Set the visibility for '2007-07 Schweizer Ferien' and its subfolders.
Please respect our guidelines.

Private
Only you have access to this folder.

Shared
Friends: – Select...
Password: – Set...

Public
All content of public folders and their subfolders is visible to anyone.

Cancel | Save

Share

wuala by LACIE

Wuala Beta – My Friends: Julien > NOAH & EWAN Juni 07

My Files | My Friends | My Groups | World

My Friends Search

NOAH & EWAN Juni 07

Julien

Views 456
Comments 0
Favorited 0 times
Linked 0 times

DSC02283 DSC02297 DSC02355 DSC02364 DSC02398 DSC02409

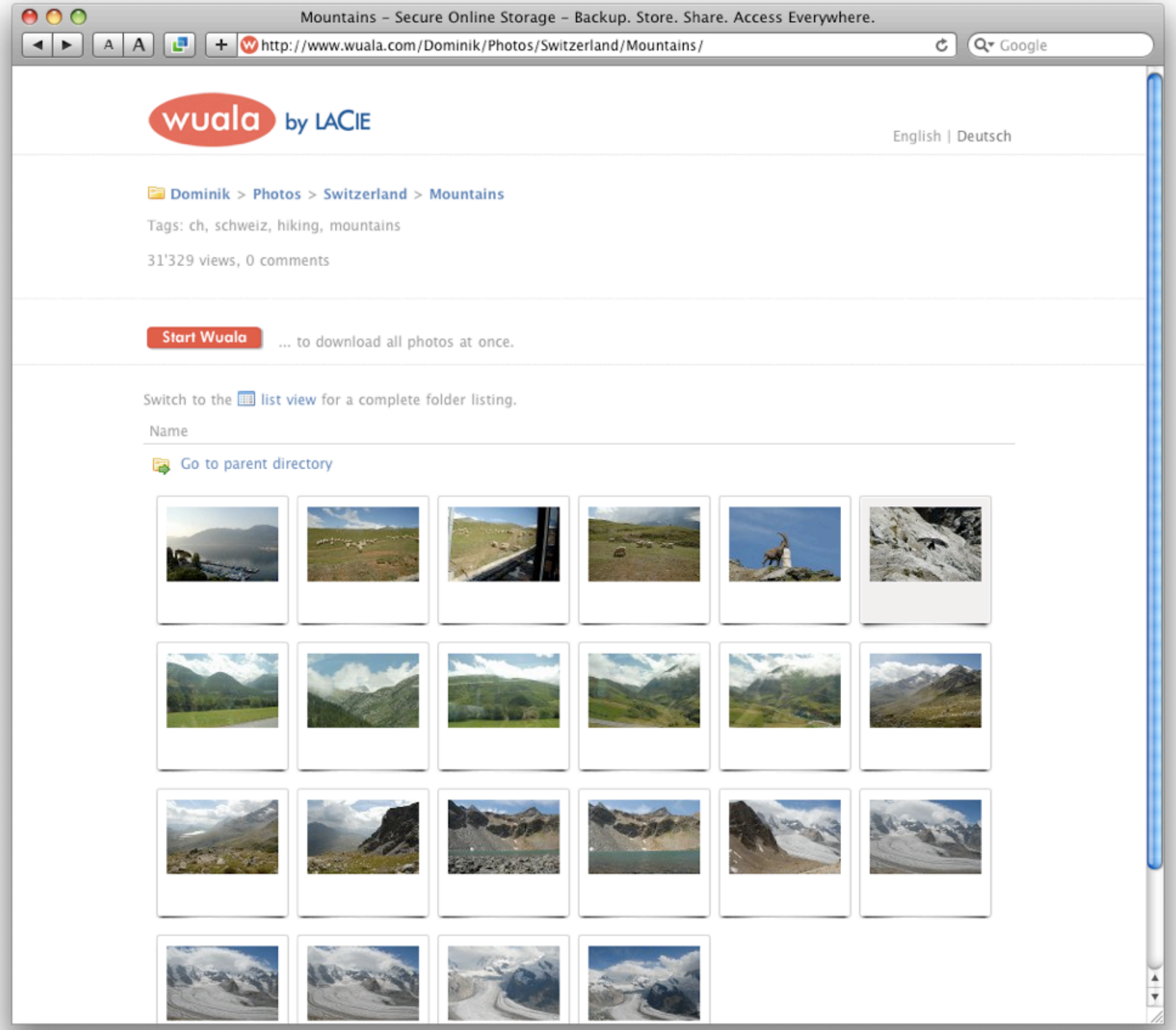
35 KB/s 0 KB/s Maintaining DSC08450.JP

DSC02297.jpg

Previous Next Zoom Move Select Slideshow Sidebar

Web Links

wuala by LACIE



Groups

wuala by LACIE

Wuala Beta – My Groups: Wuala – Team

My Files | My Friends | My Groups | 4 New | My Groups Search

Wuala – Team
Das Team
Click here to add tags
Click here to specify your website

Type: Private | Members 11
Founder: Dominik | Views 30219
Created: Apr 29, 2008 | Comments 0
Your Role: Admin | Linked 2 times

Files in 'Wuala – Team' (16)

Business, Content, Development, Ideas, LaCie, Marketing and Communications, Organisation, Quality Assurance

Resources, Roadmap, Server, Technology, Trash, UI, Website, Quote of the Day

Recently viewed – show more

Admin (7)

Carola Admin, Dominik Grolimund (Dominik) Admin, fabius Admin, Luzius Admin, oona Admin, Roger Admin, Sushi Admin

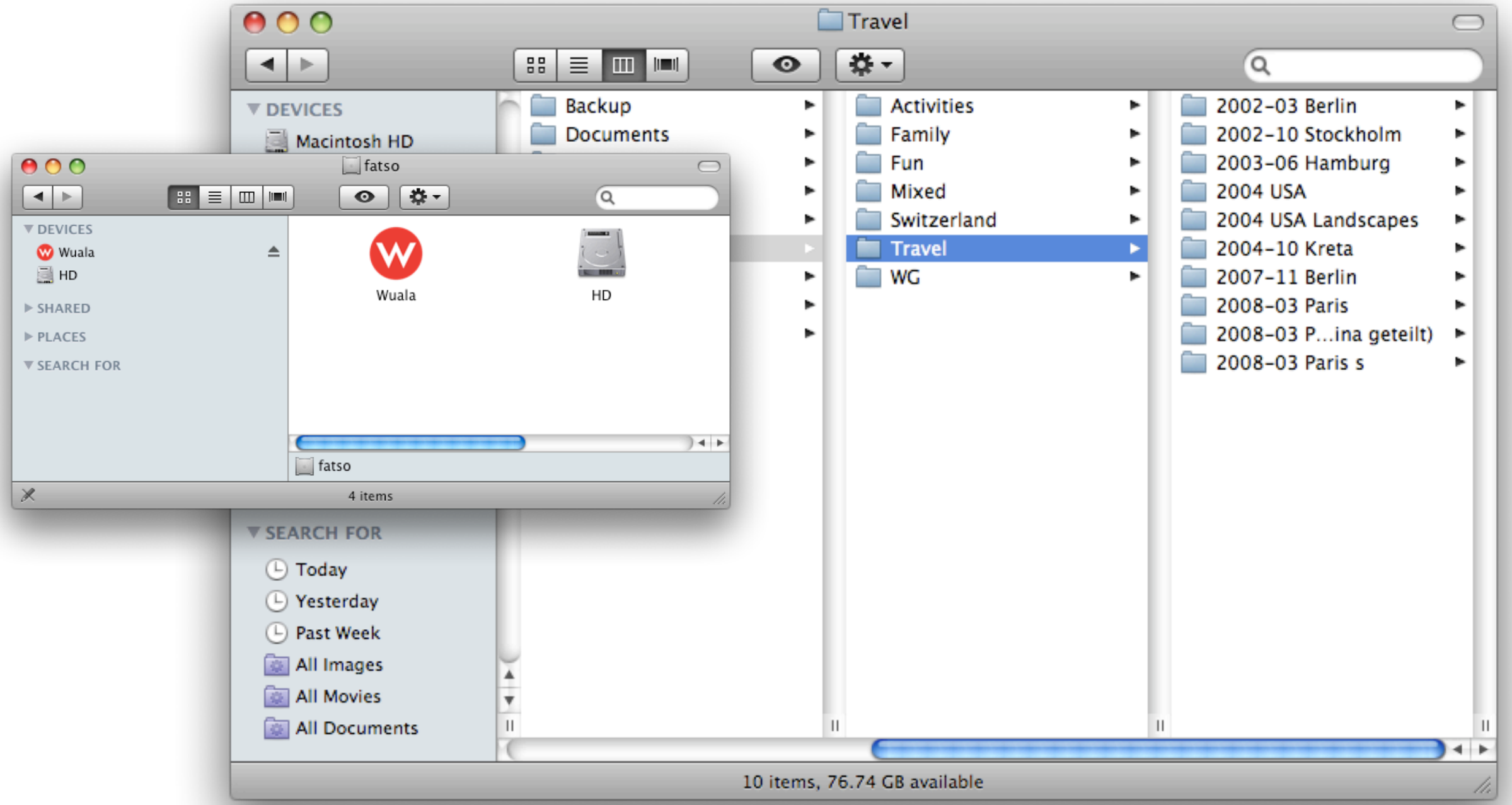
Member (4)

Alexander Schwab (cborealis) Member, hypnotortoise Member, Thomas (tmaeder) Member, Marius Bürki (verbalkiter) Member

12 KB/s | 0 KB/s | 382 GB of 634 GB used (get more) | Dominik

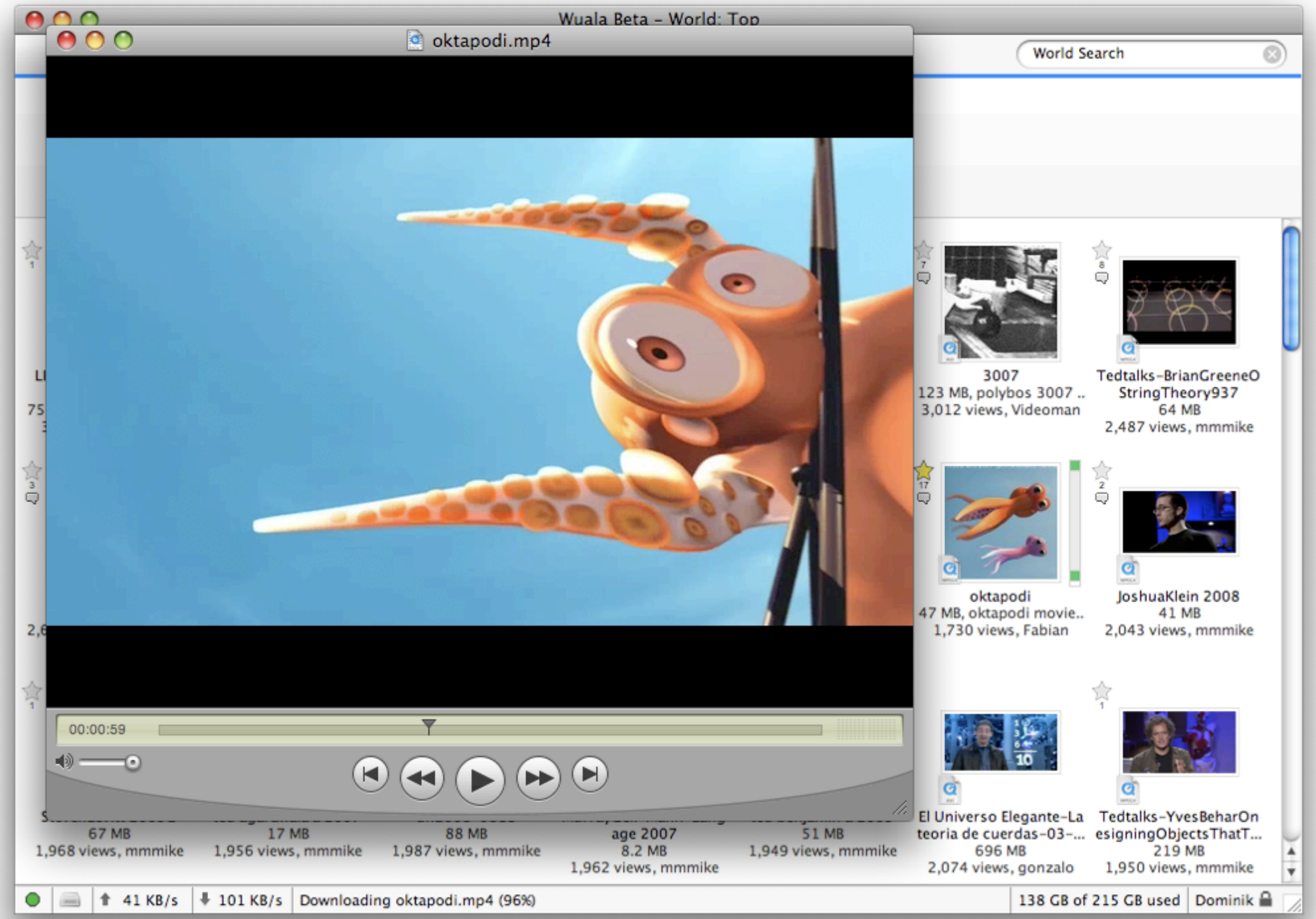
Network Drive

wuala by LACIE



Stream

wuala by LACIE

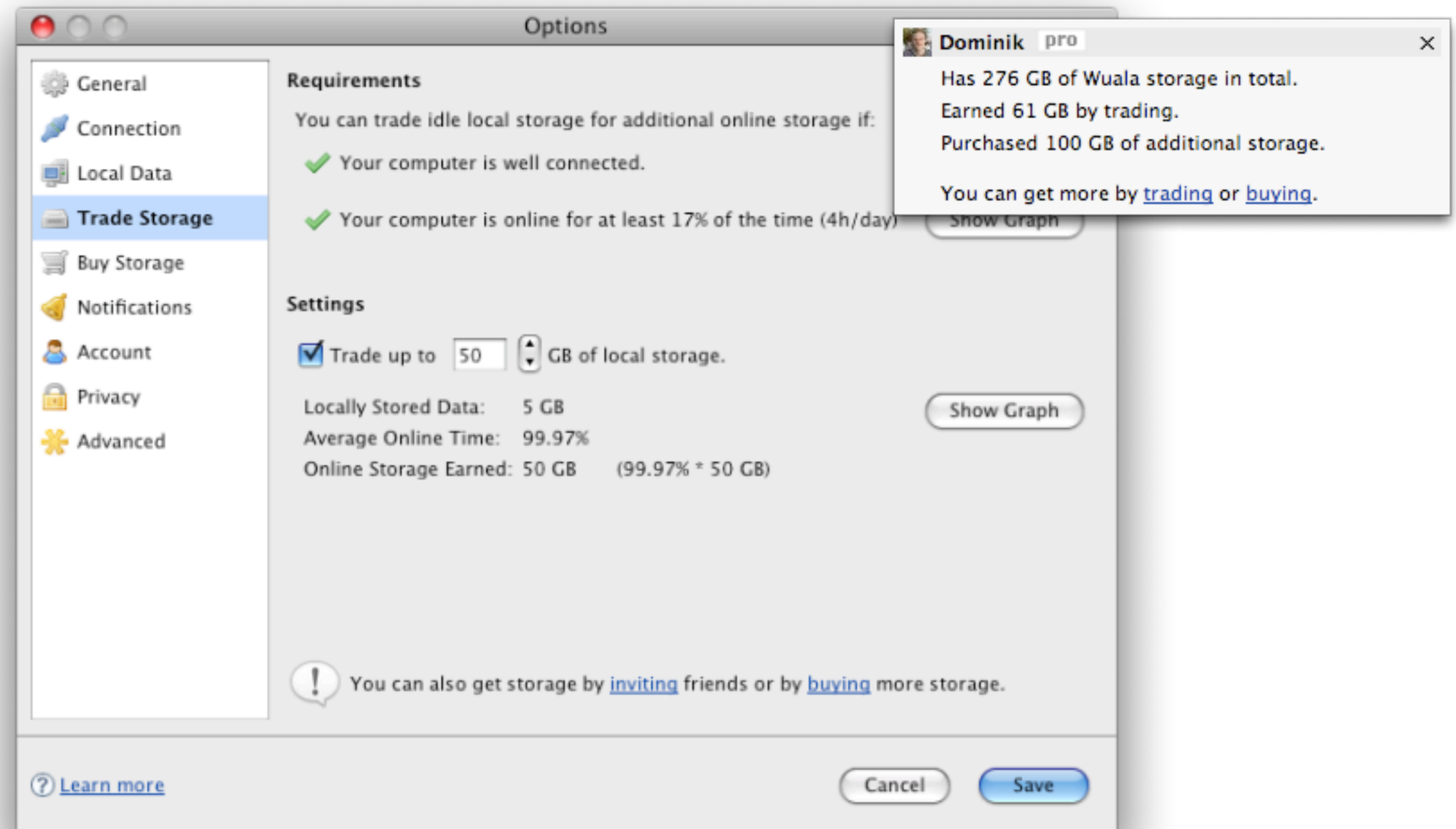


Trading Storage

wuala by LACIE

Turn local storage into secure and reliable online storage

For trading, one needs to be online 4 hours a day (running average)



Features

wuala by LACIE

Start with 1 GB of storage

Get more storage by

- trading local disk space storage for online storage
- buying additional storage

Encrypted

No file size limits

No traffic limits

Fast downloads

Streaming

Differentiation

Architecture

wuala by LACIE

On the users' computer:

Roadshow.mpg (60 MB)

1. Encrypt (AES 128)

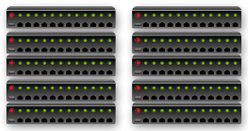
2. Erasure code (Reed Solomon)

3. Upload meta data to our servers

4. Upload fragments to:
   - Fragment servers (ex: 140)
   - Grid network (ex: 300)

Our data center:

Meta servers



Content servers

Fragment servers

On another computer:

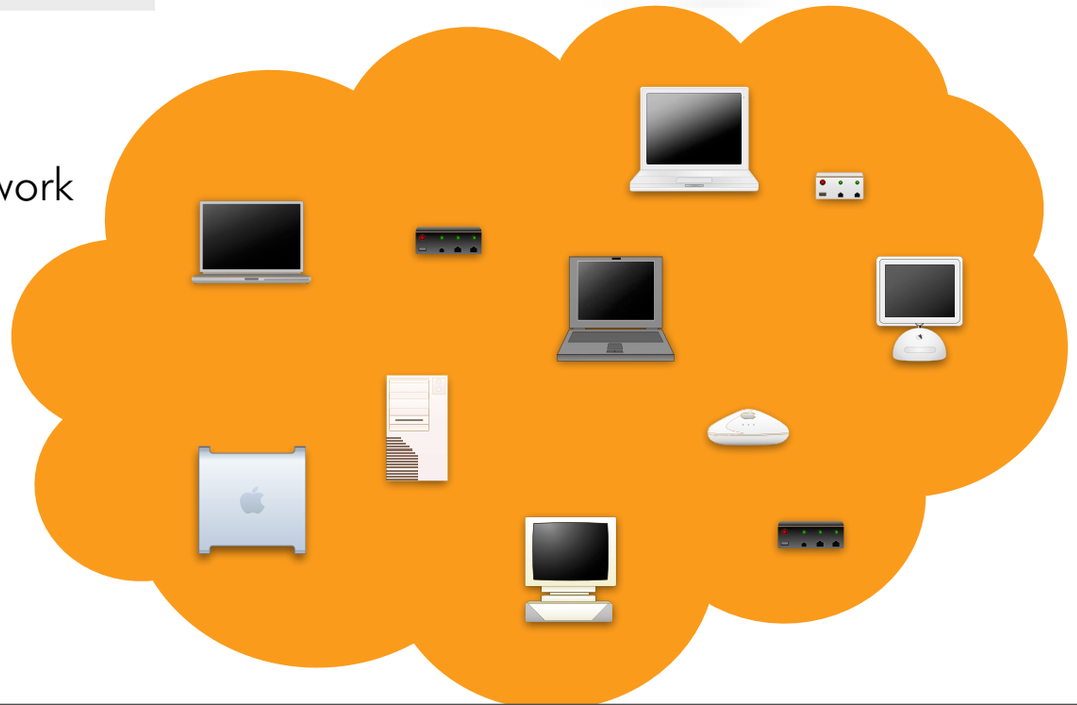
Roadshow.mpg (60 MB)

3. Decrypt (AES 128)

2. Deconstruct

1. Download fragments from:
   - Grid network (ex: 97)
   - Fragment servers (ex: 3)

Grid network



Security and Privacy

wuala by LACIE

All data gets encrypted on YOUR computer

Your password never leaves your computer

No one unauthorized, including us, can access your files

This is in stark contrast to services who have access to customers' data

Vision

Distributed Storage

wuala by LACIE

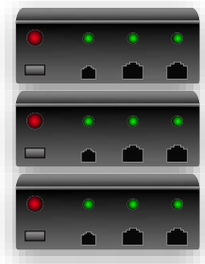
A cloud of devices

NAS, PCs, and servers

A distributed storage system

Professionals

Home users



Home users

Organizations

Universities

Technology

data stored in the p2p network

users's computer can be offline

how to ensure availability
(persistent storage)?

two approaches

1. make sure the data is always in the network

move the data when a computer goes offline

bad idea for lots of data and high churn rate

2. introduce redundancy

redundany = replication?

$$p_{rep} = 1 - (1 - p)^k$$

p = node availability

k = redundancy factor

p_{rep} = file availability

redundany = replication?

$$p_{rep} = 1 - (1 - p)^k$$

example

$p = 0.25$

$k = 5$

$p_{rep} = 0.763$ ⟶ not enough

redundany = replication?

$$p_{rep} = 1 - (1 - p)^k$$

example

p = 0.25

k = 24 ⟶ unrealistic

p_{rep} = 0.999

erasure codes

encode m fragments into n

need **any** m out of n to reconstruct

reed-solomon (optimal codes)

RAID storage systems

(vs. low-density-parity-check need (1+e) * m,

where e is a fixed, small constant)

availability

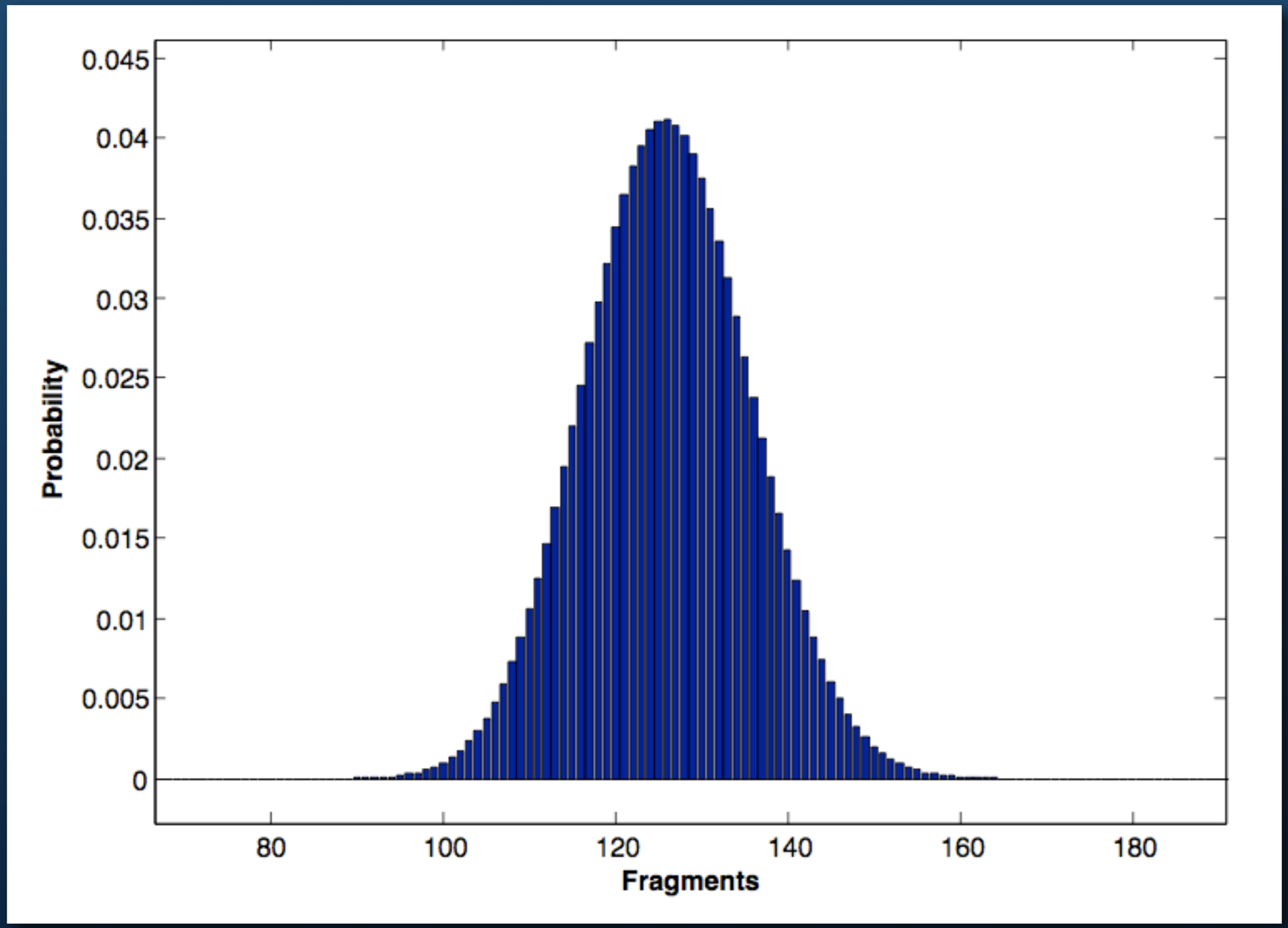
$$p_{ec} = \sum_{i=m}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

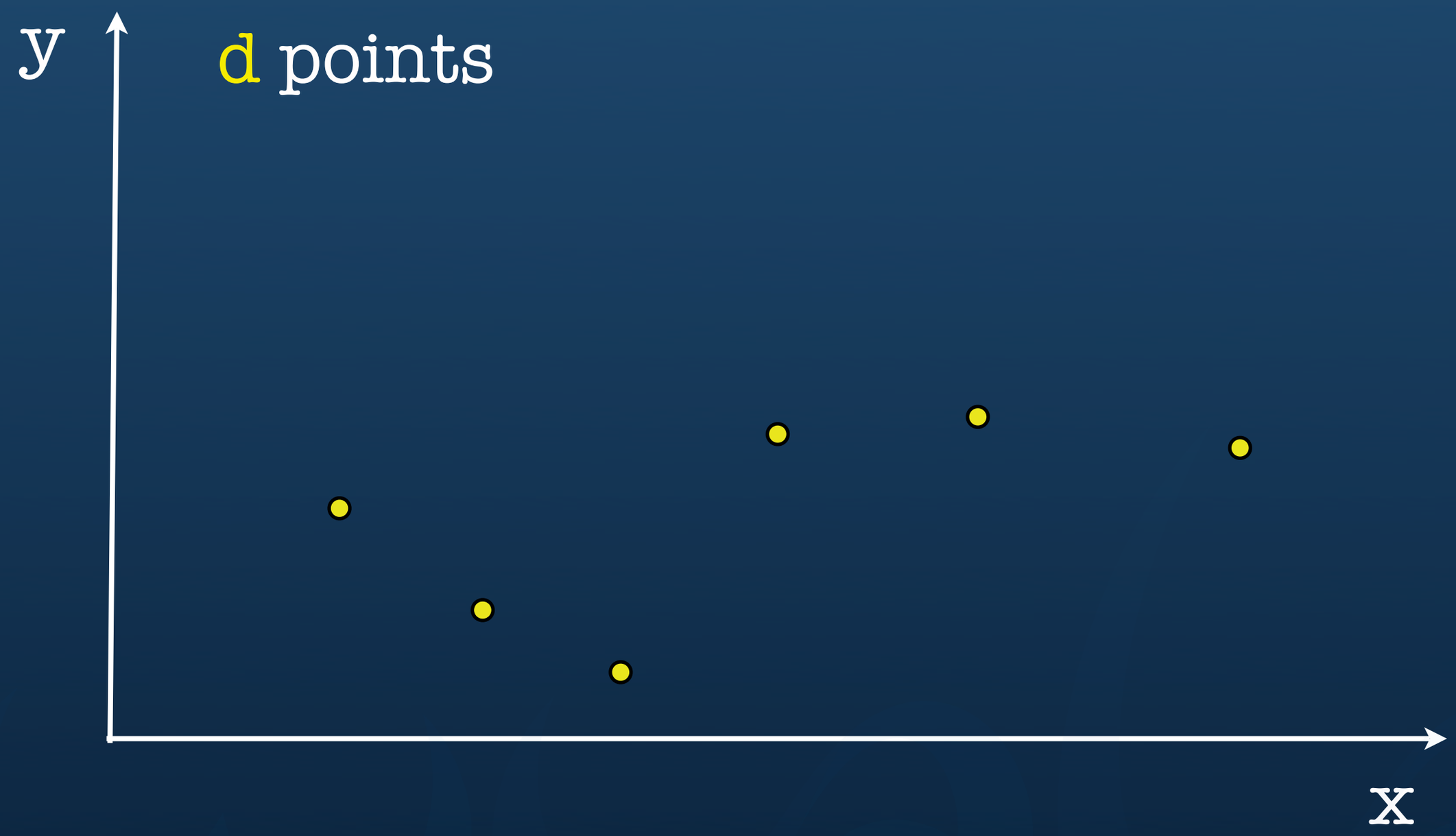
$p = 0.25$

$m = 100$, $n = 517$, $k = n/m = 5.17$

$p_{ec} = 0.999$

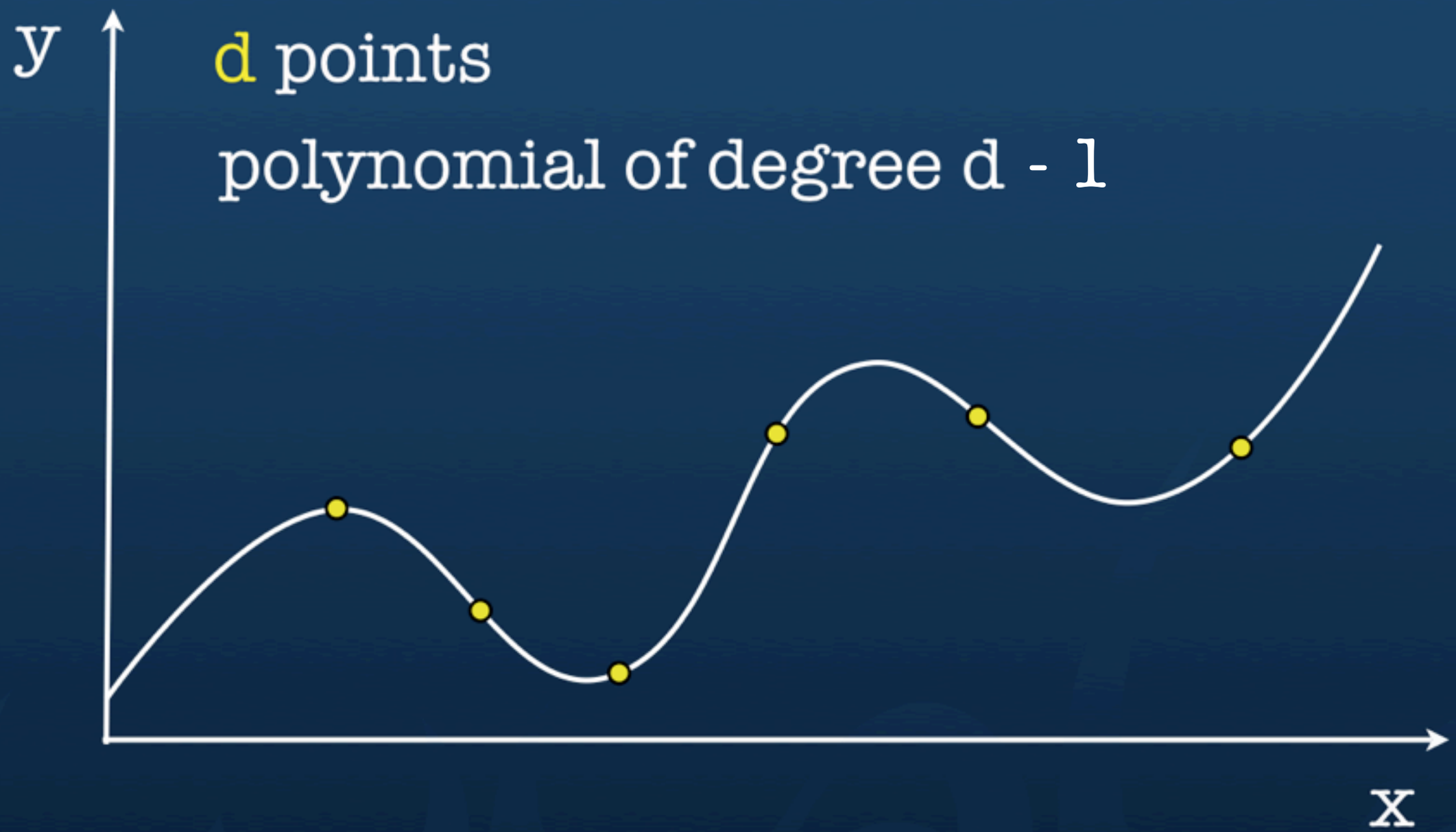
$k = n/m = 5.17$ vs. $k = 24$ using replication


0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
Probability
80
100
120
140
160
180
Fragments


y
d points
x

d points

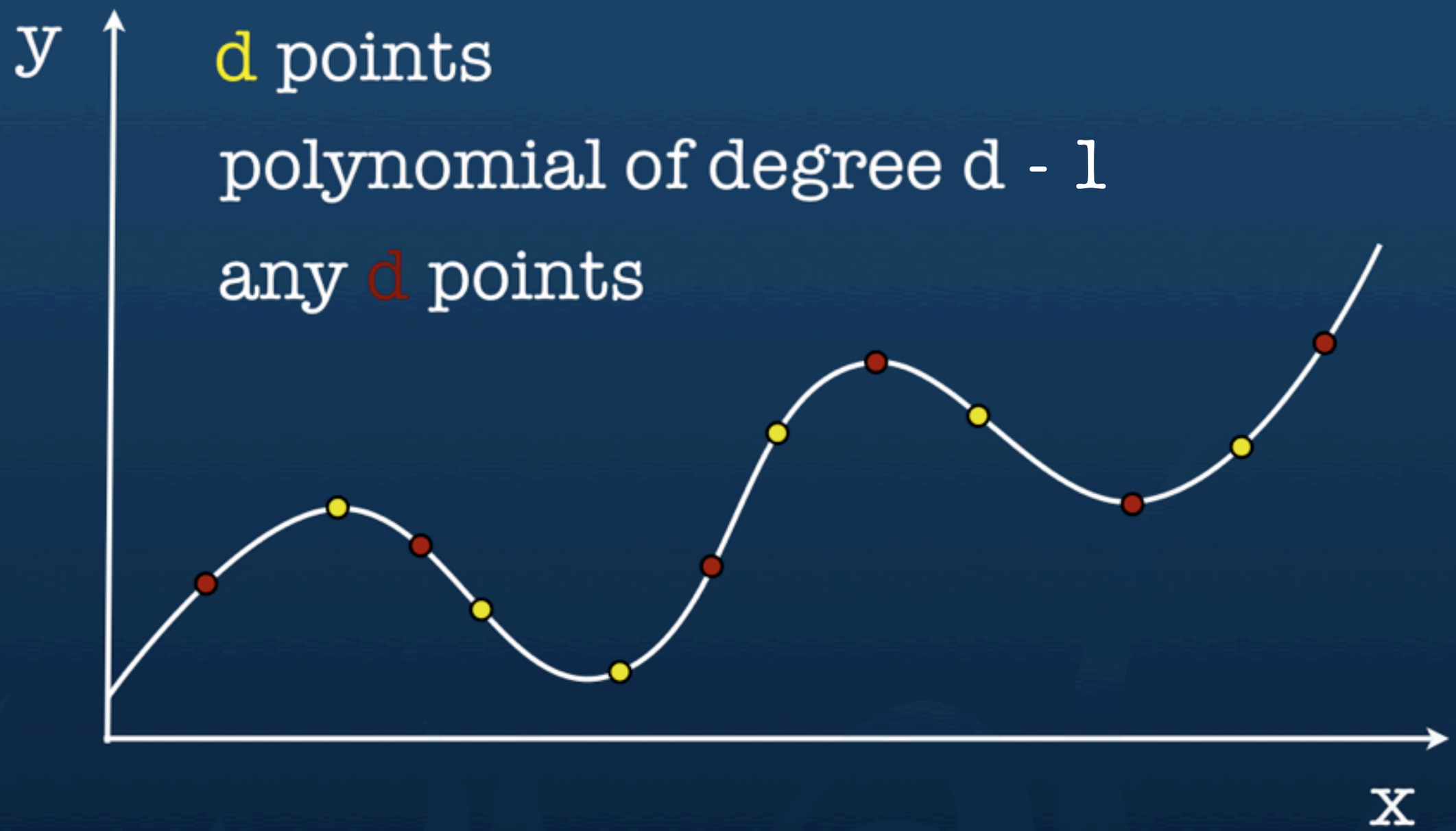
polynomial of degree d - 1



d points

polynomial of degree d - 1

any d points



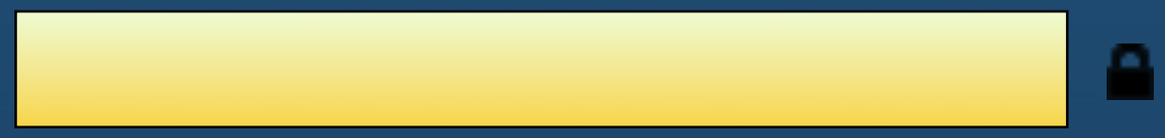
alice stores a file

roadtrip.mpg

alice drags roadtrip.mpg into wuala

1. encrypted on alice's computer (128 bit AES)

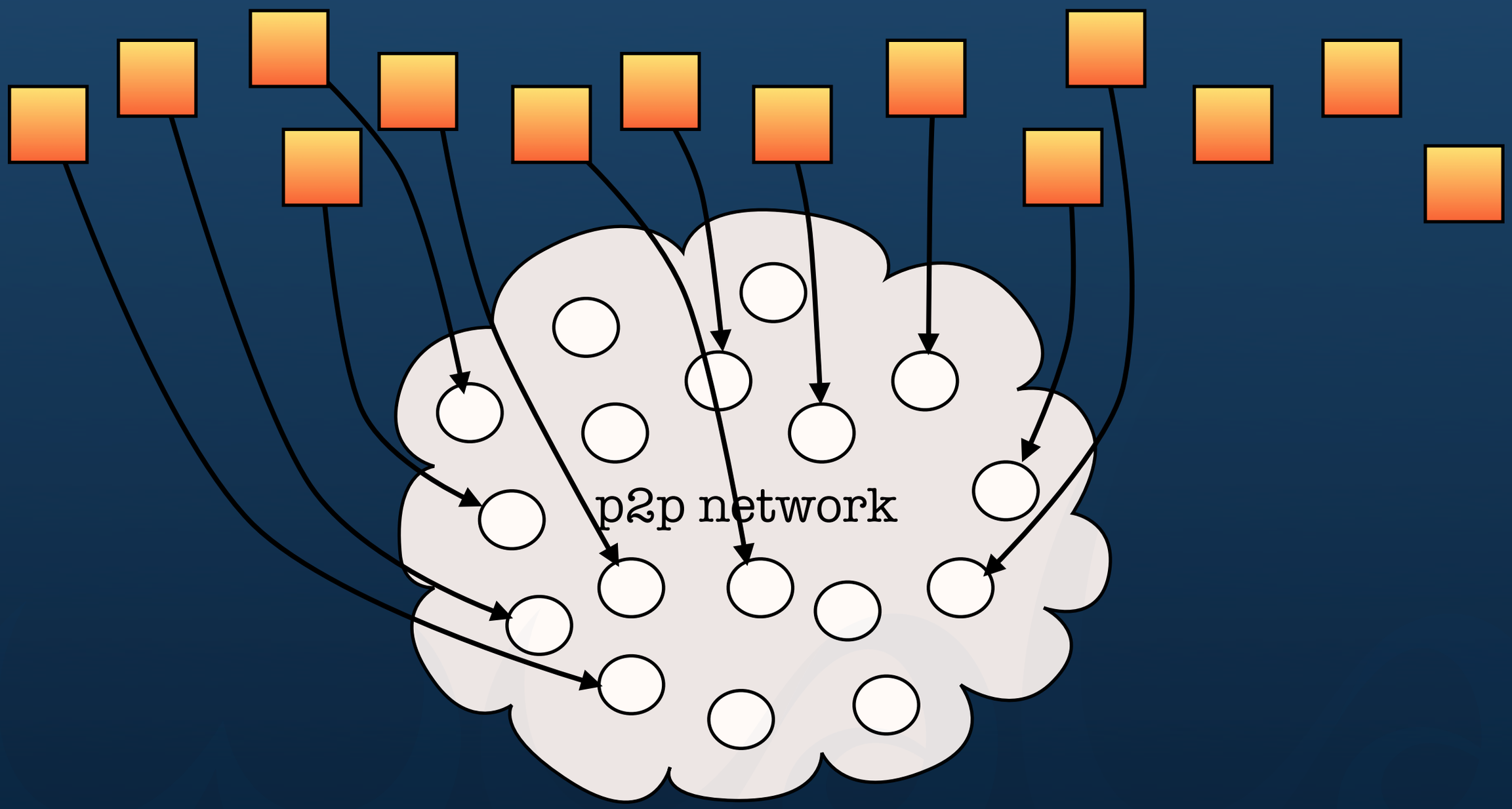
1. encrypted on alice's computer (128 bit AES)



2. encoded into redundant fragments

1. encrypted on alice's computer (128 bit AES)

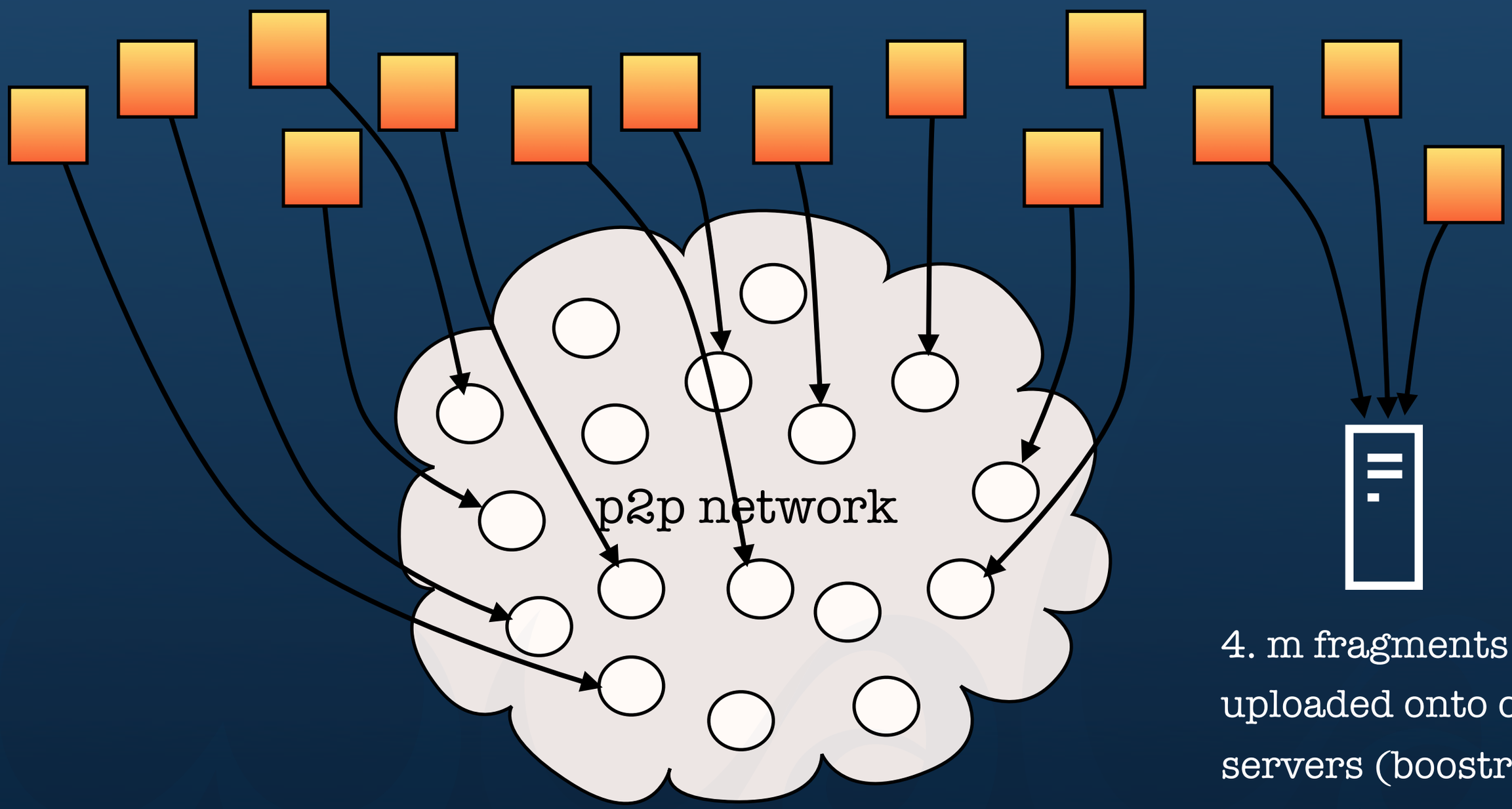
2. encoded into redundant fragments



3. uploaded into the p2p network

1. encrypted on alice's computer (128 bit AES)

2. encoded into redundant fragments



4. m fragments uploaded onto our servers (boostrap, backup)

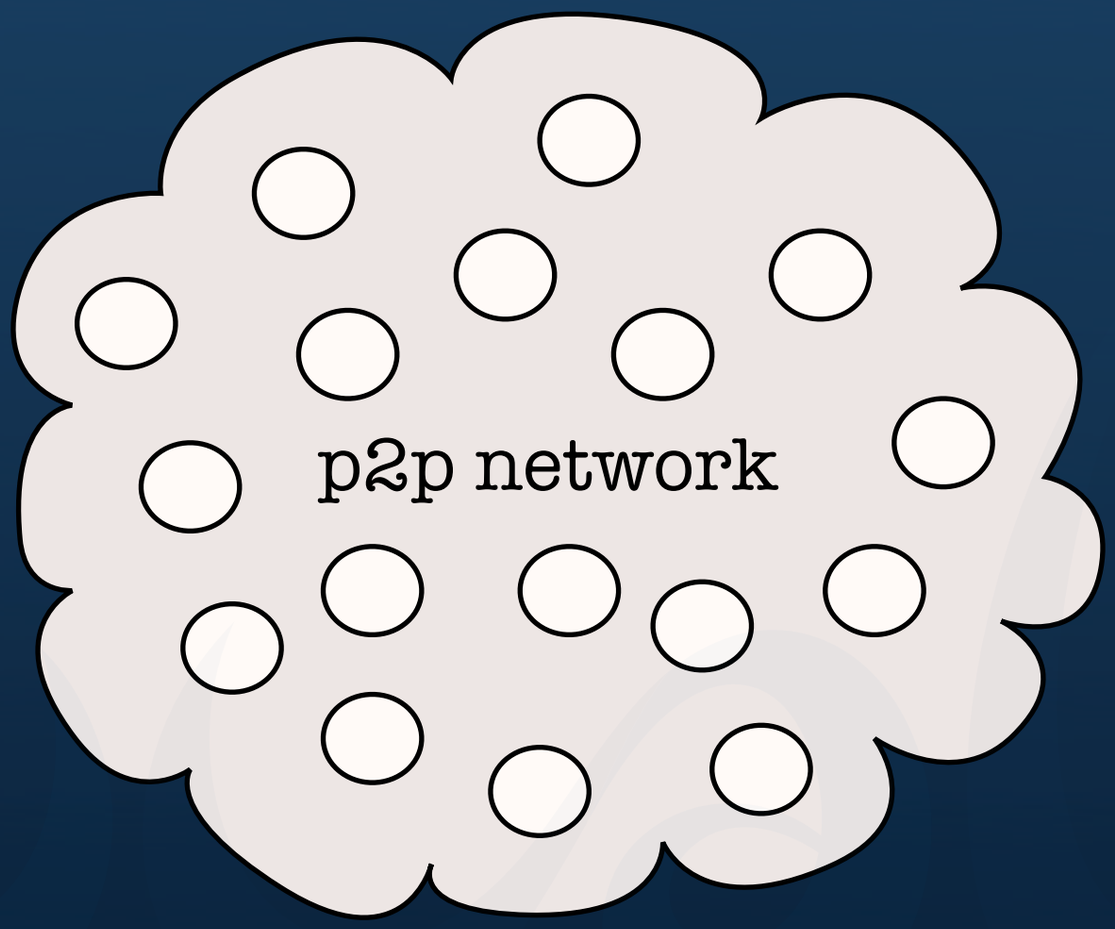
3. uploaded into the p2p network

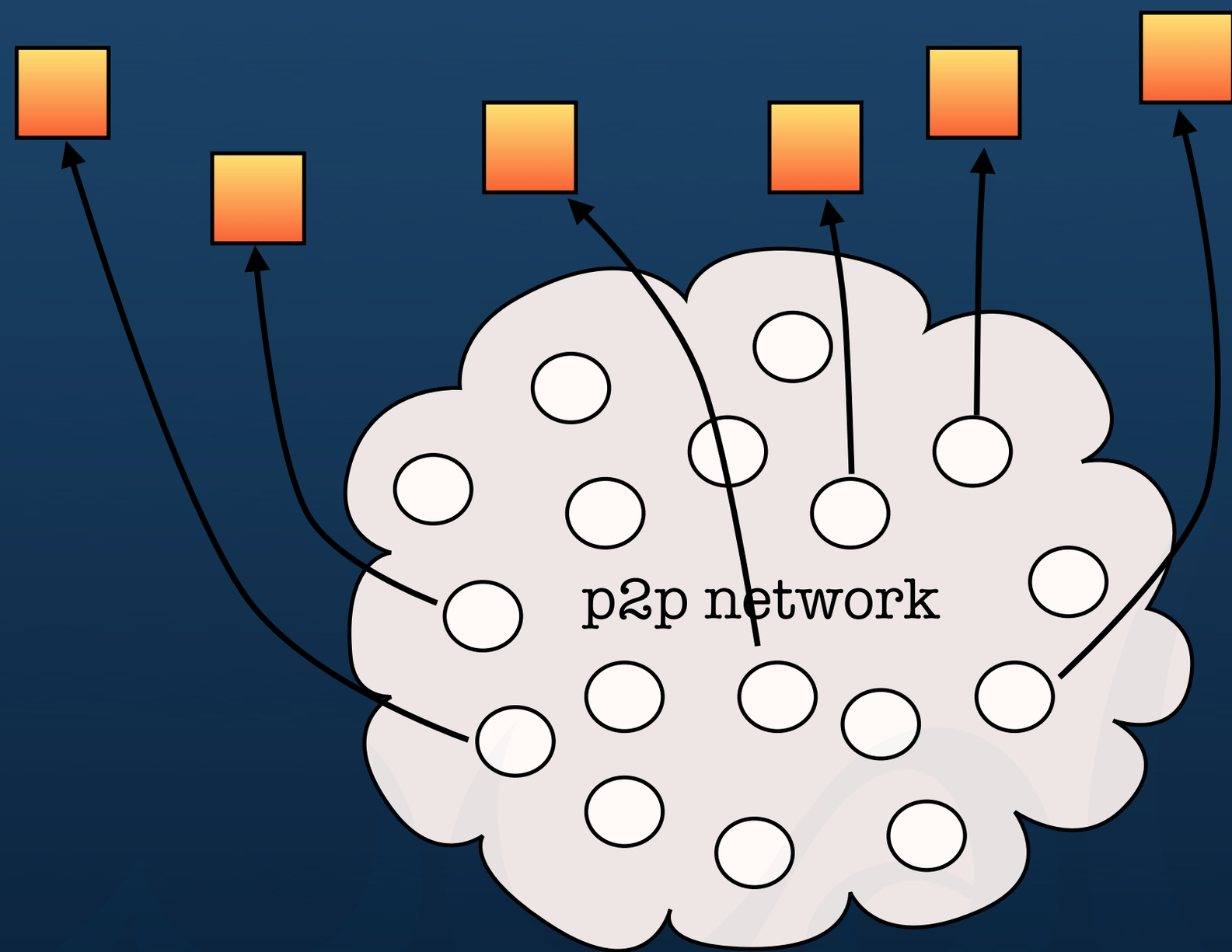
alice shares the file with bob

alice and bob have friendship key

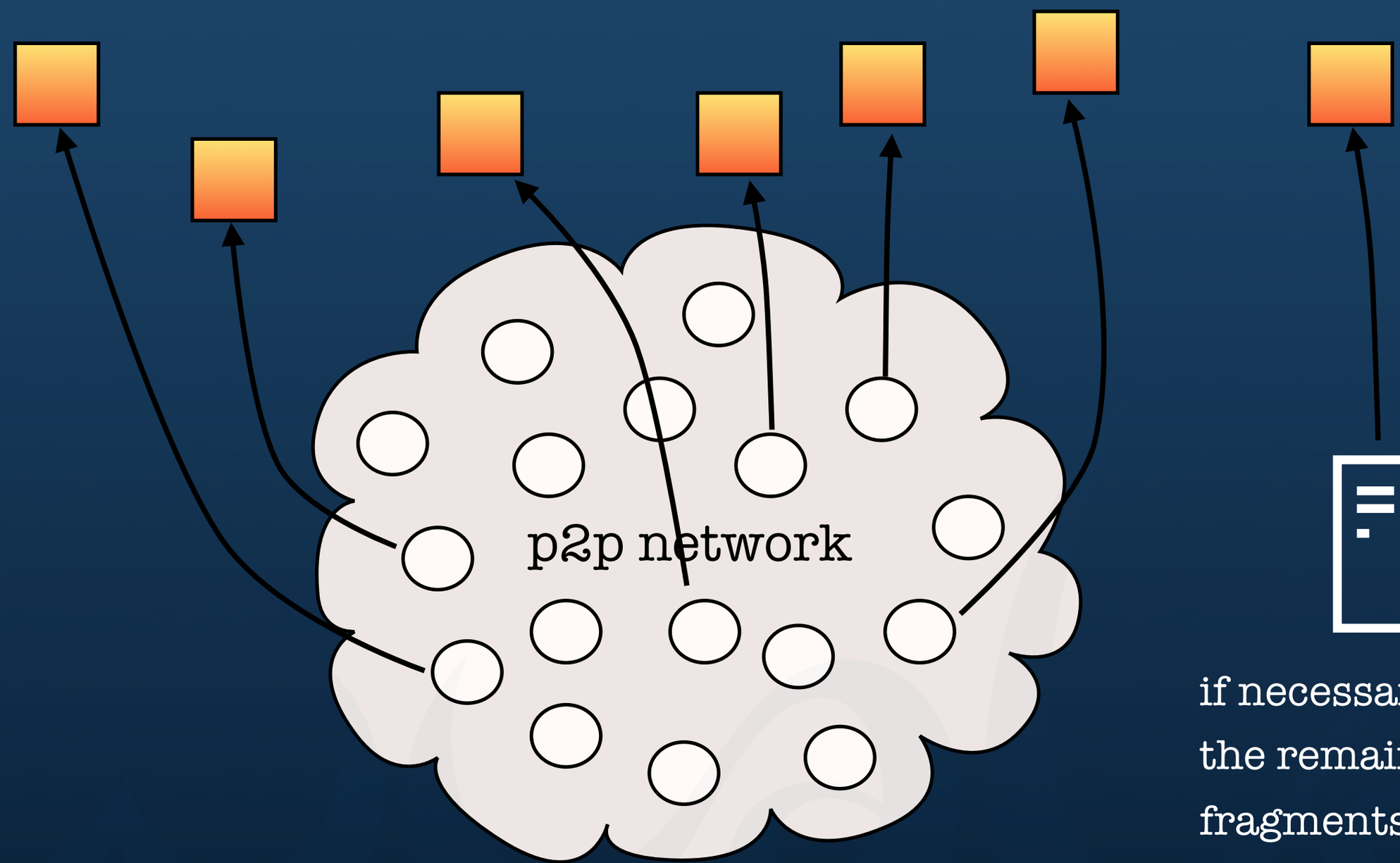
alice encrypts file key and exchanges it with bob

bob wants to download the file


p2p network

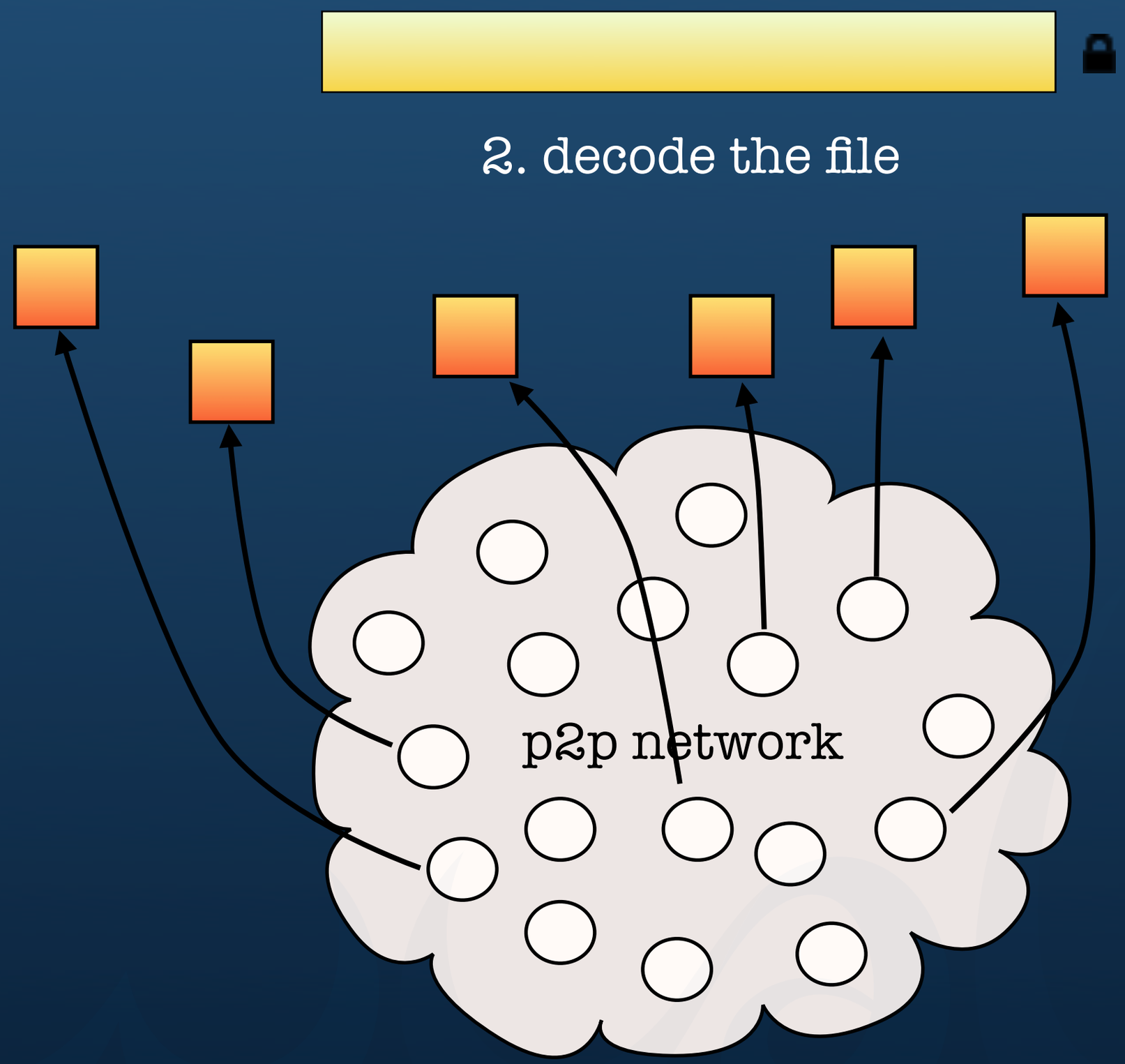


1. download subset of fragments (m)



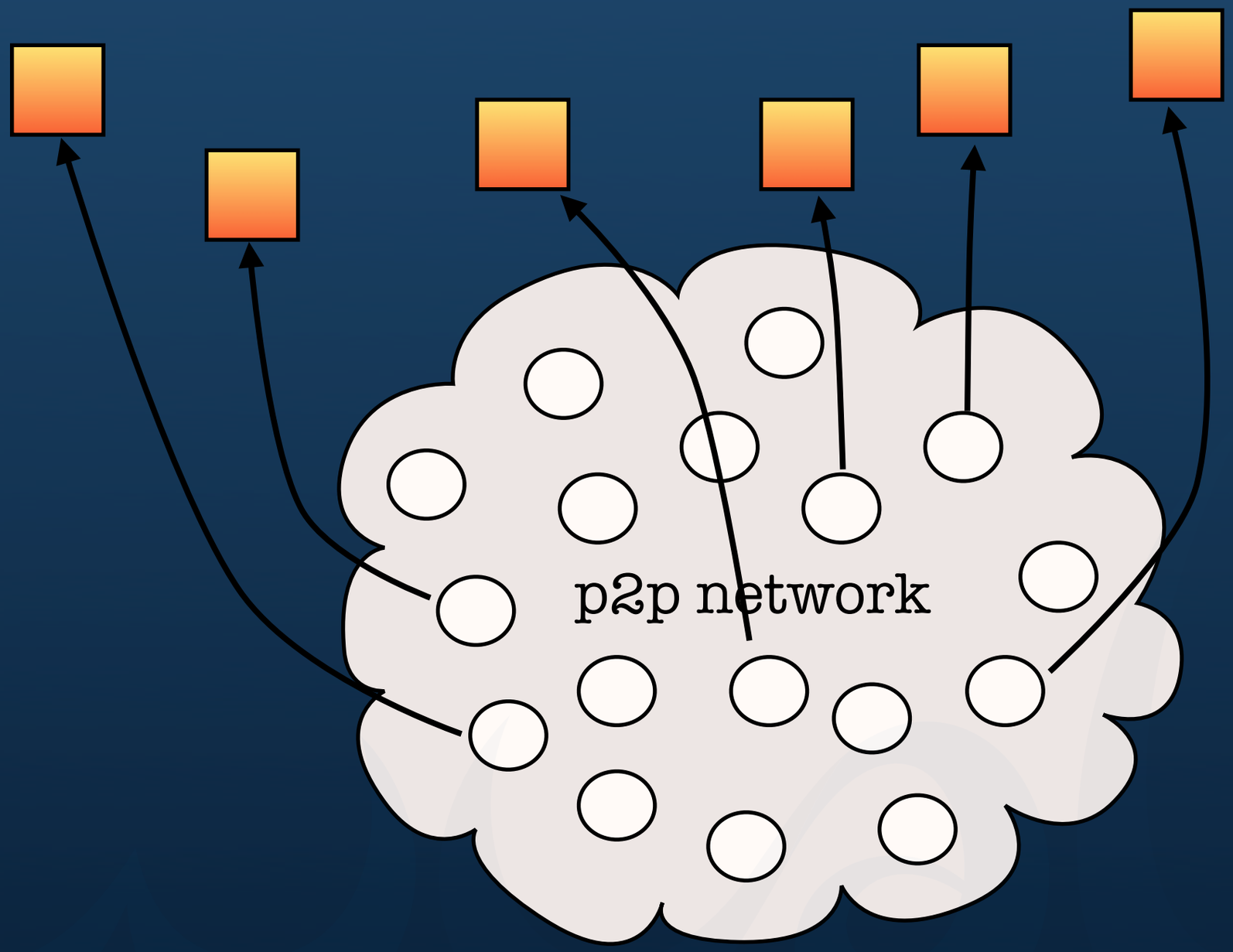
if necessary, get the remaining fragments from our servers

1. download subset of fragments (m)


2. decode the file
p2p network
1. download subset of fragments (m)

3. decrypt the file

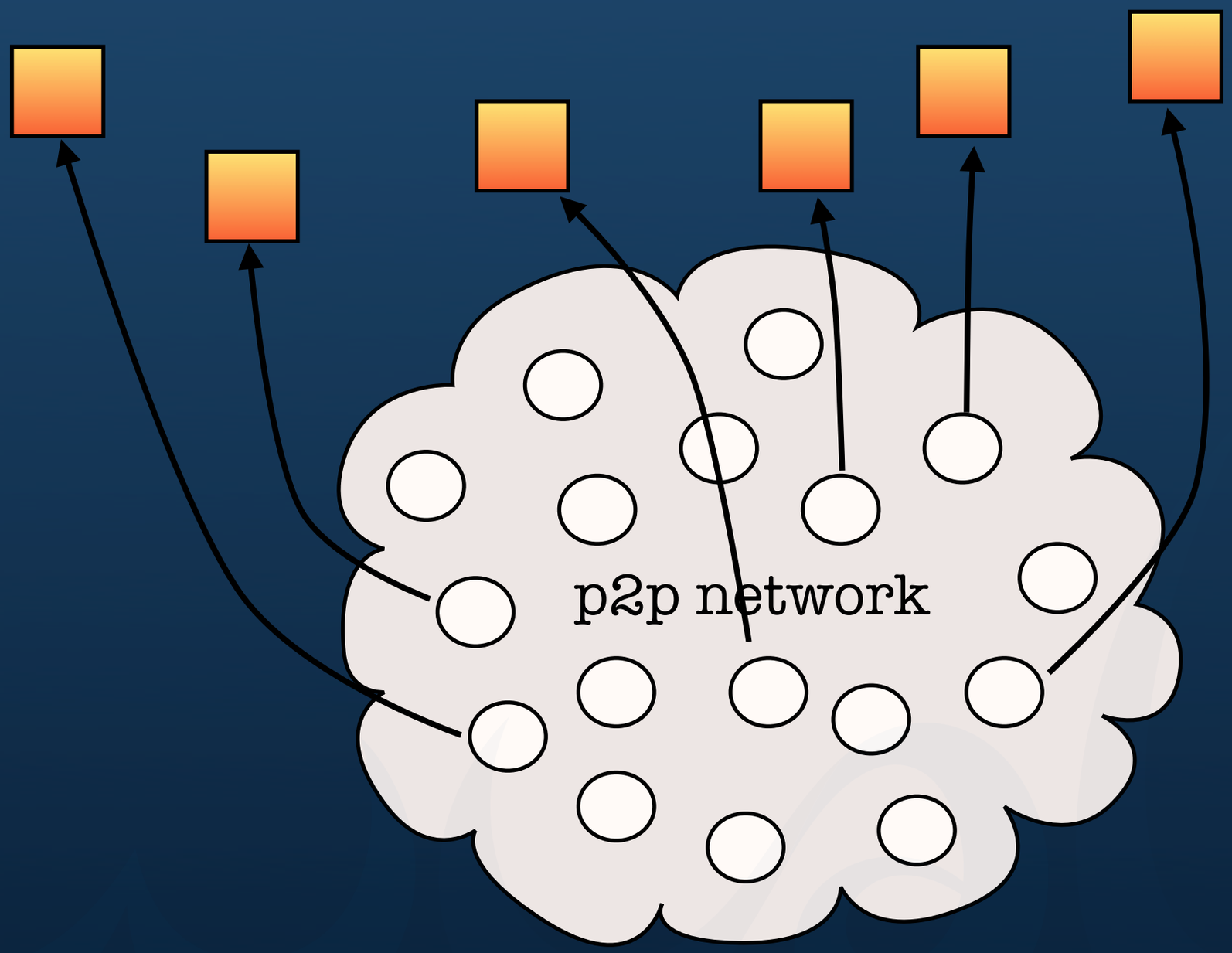
2. decode the file



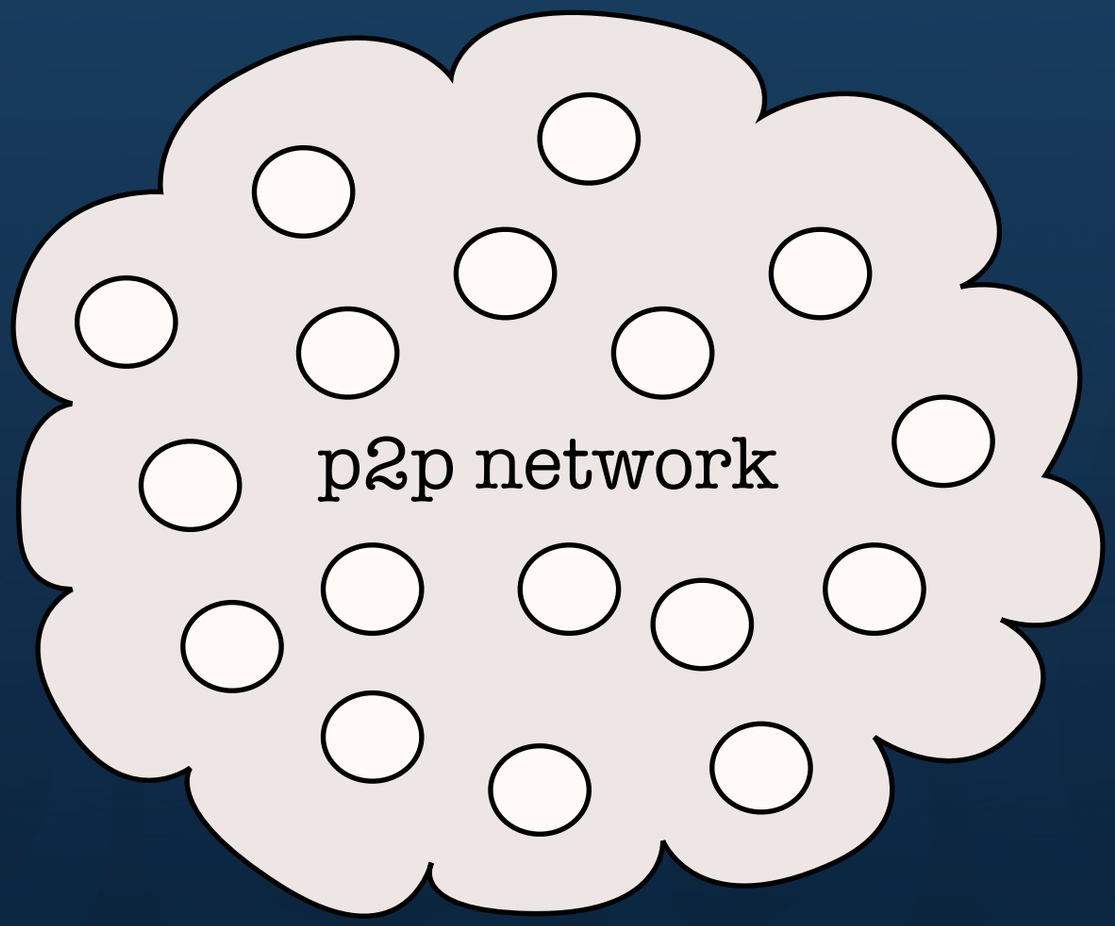
1. download subset of fragments (m)

bob plays roadtrip.mpg

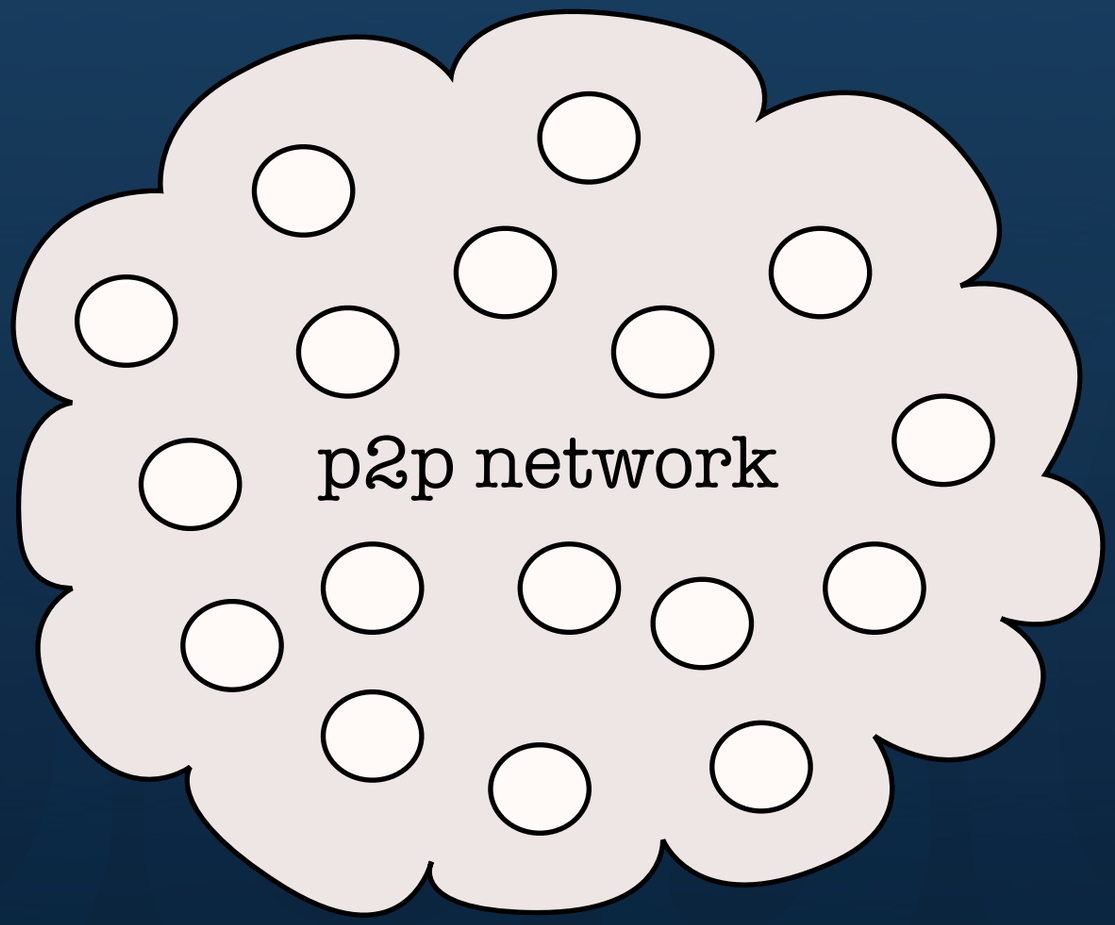
2. decode the file



1. download subset of fragments (m)

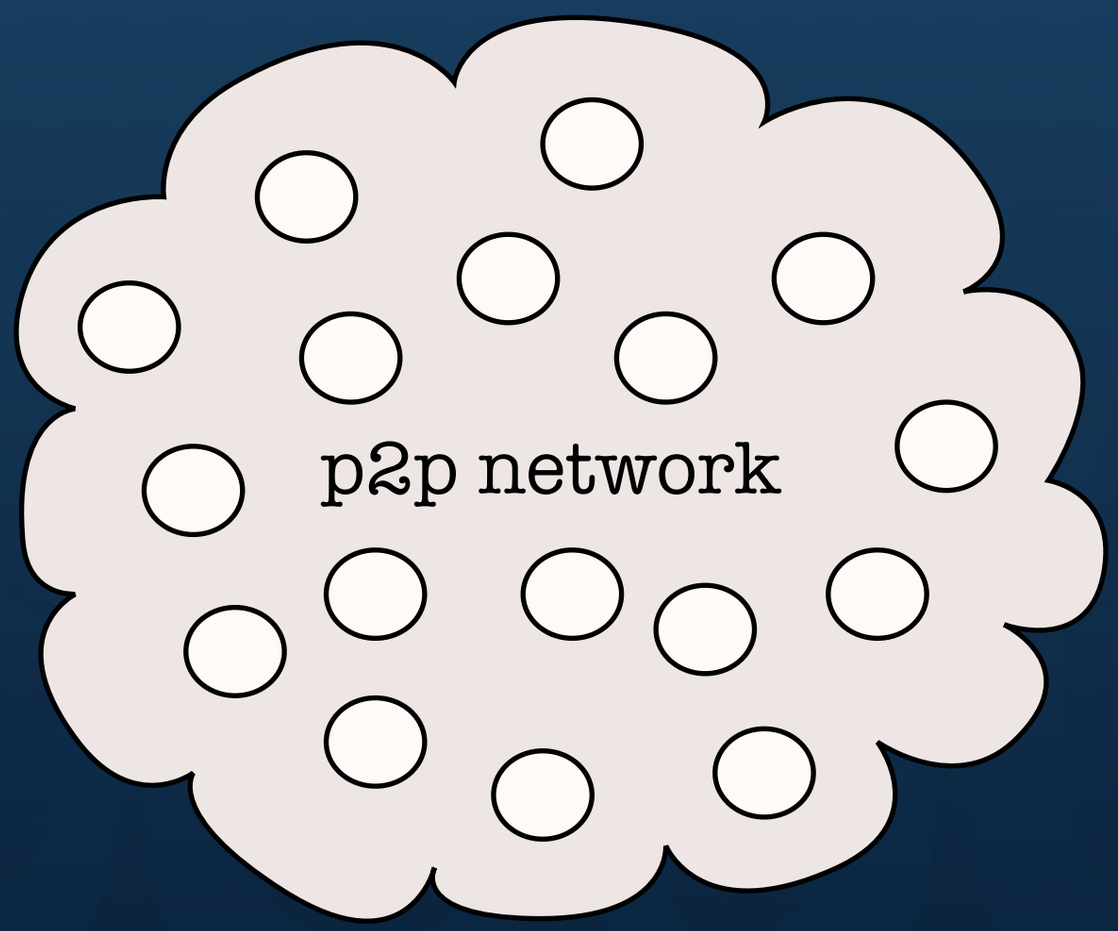

p2p network

maintenance



maintenance

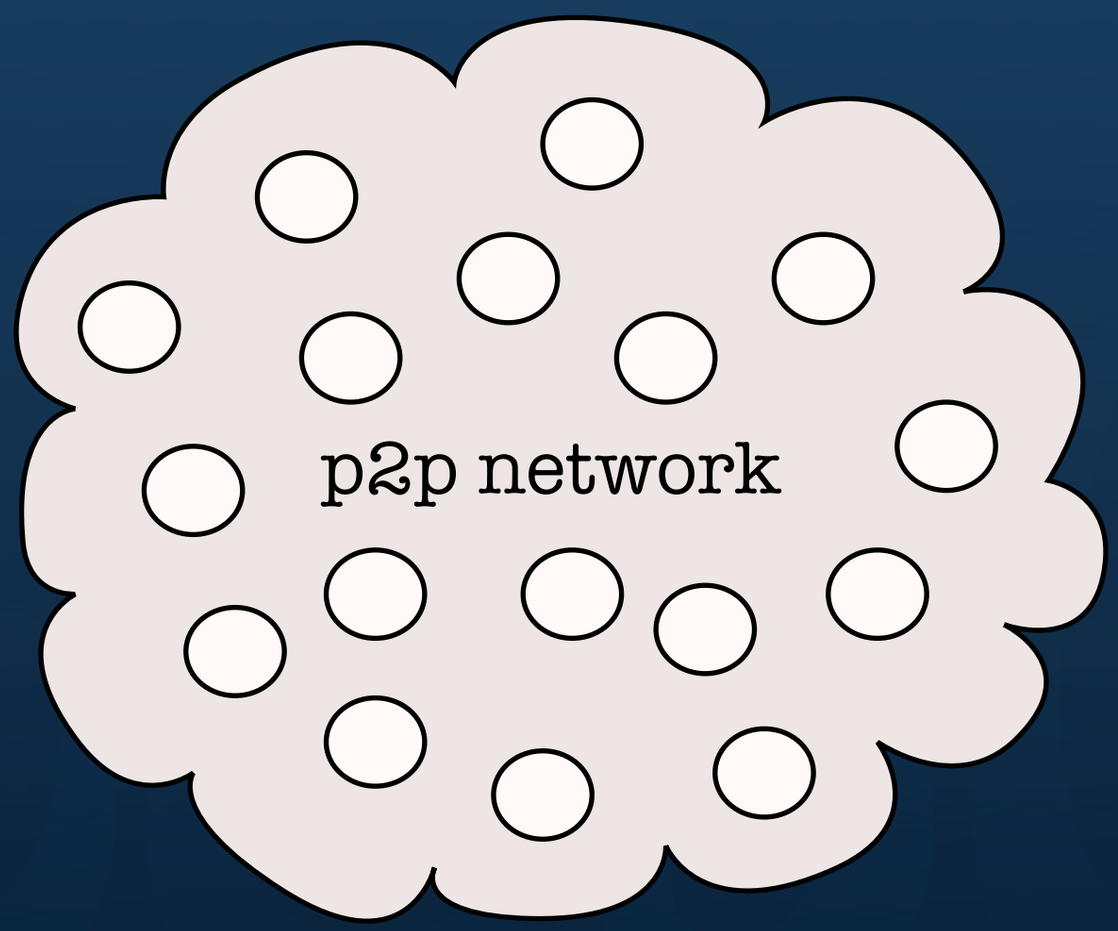
alice's computer checks and maintains her files



maintenance

alice's computer checks and maintains her files

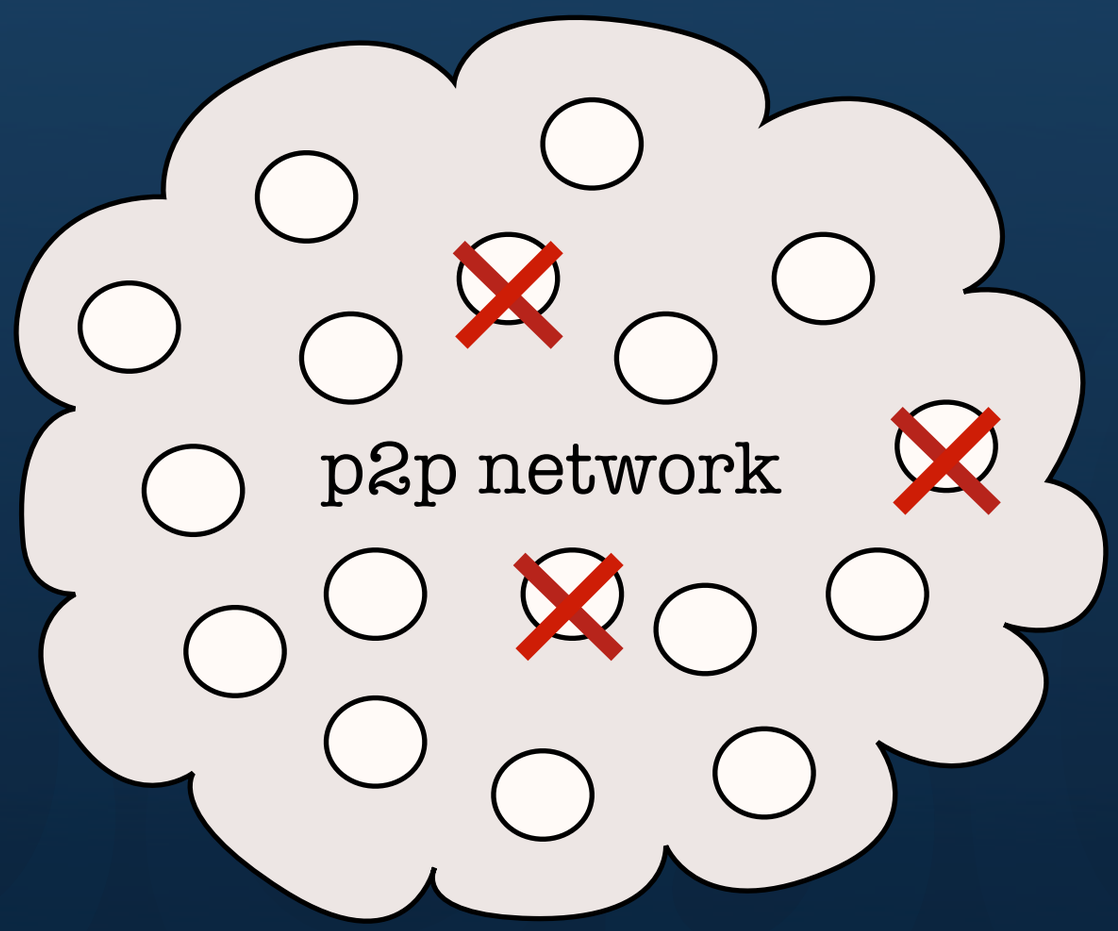
if necessary, it constructs new fragments and uploads them



maintenance

alice's computer checks and maintains her files

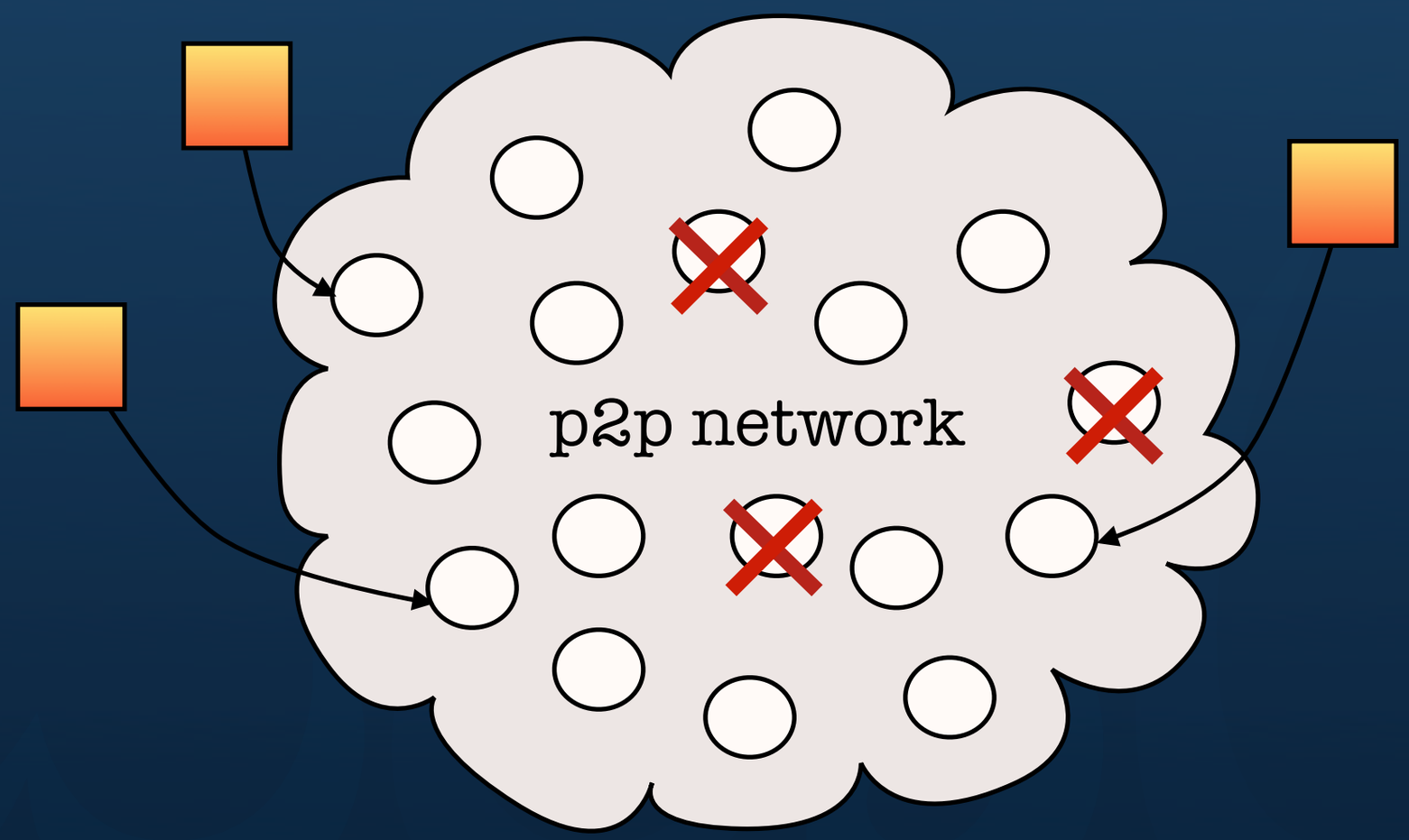
if necessary, it constructs new fragments and uploads them

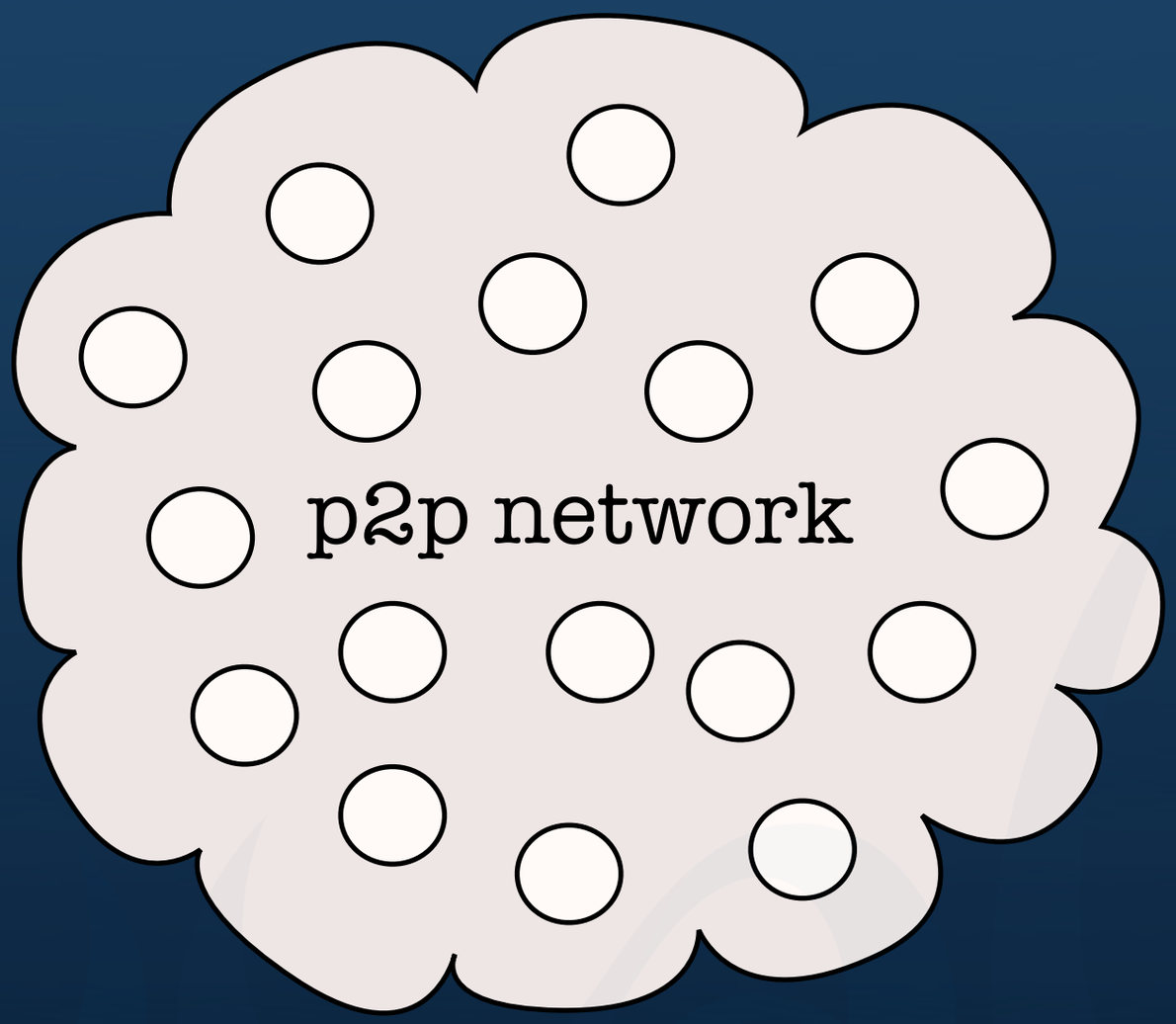


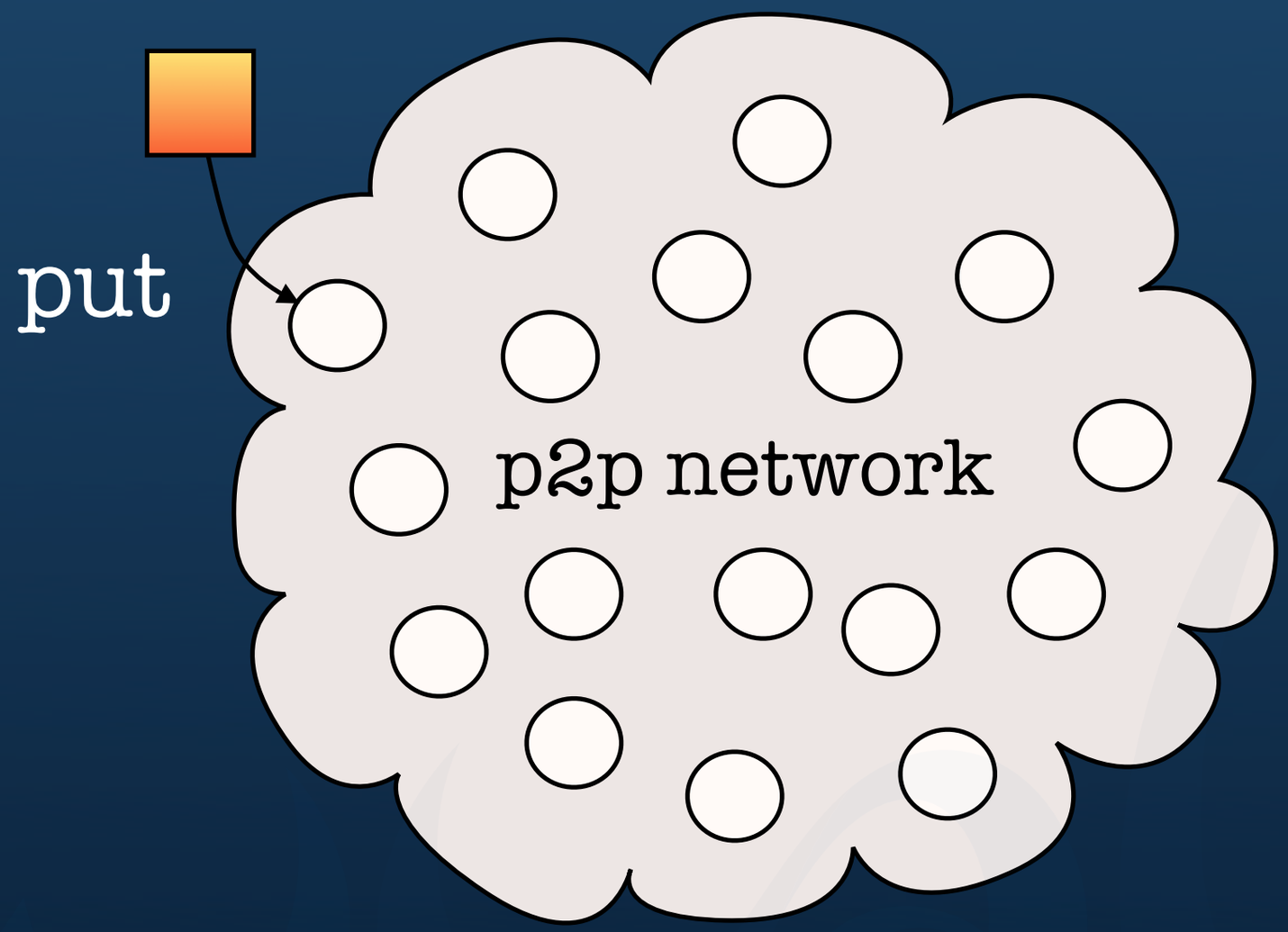
maintenance

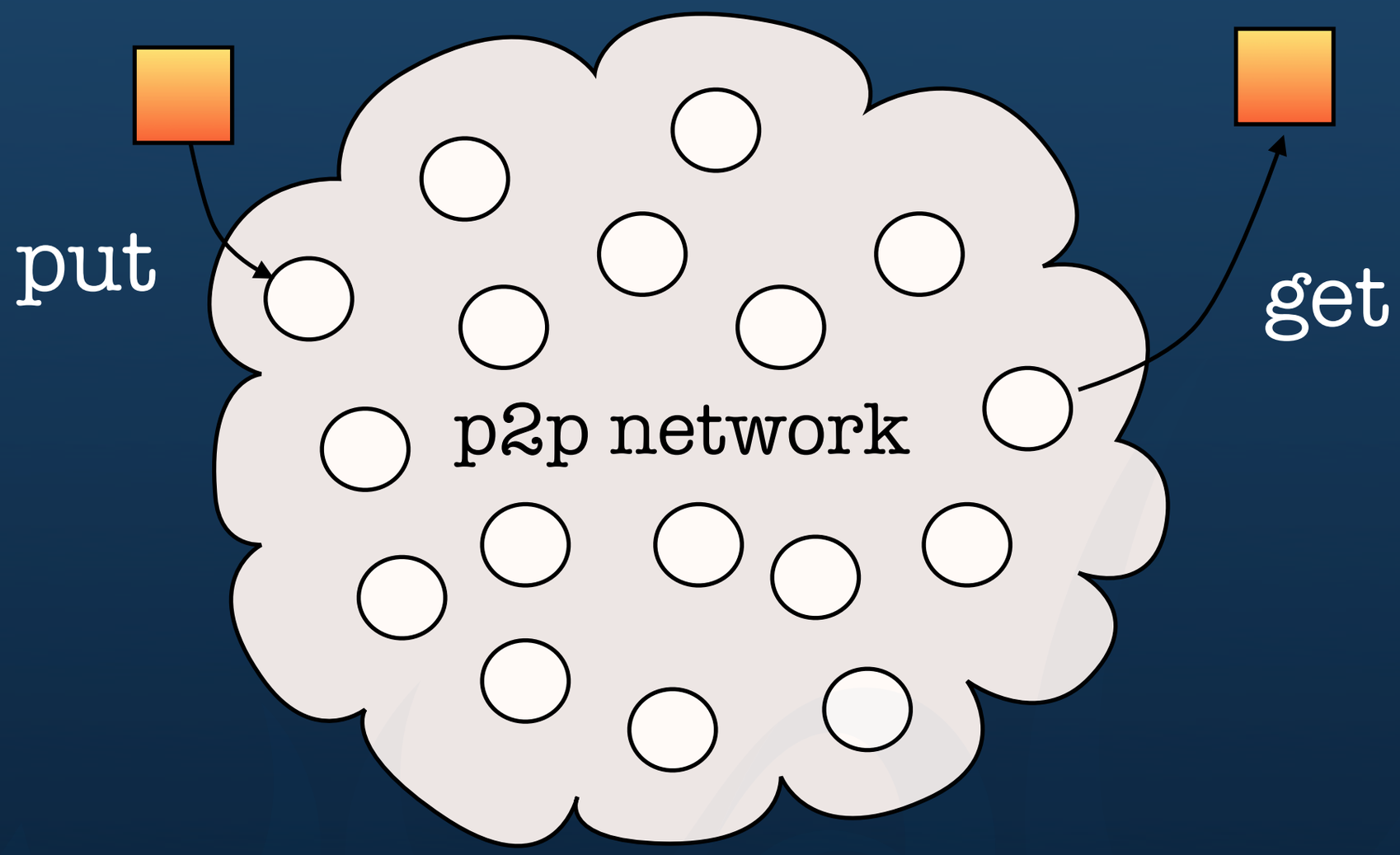
alice's computer checks and maintains her files

if necessary, it constructs new fragments and uploads them

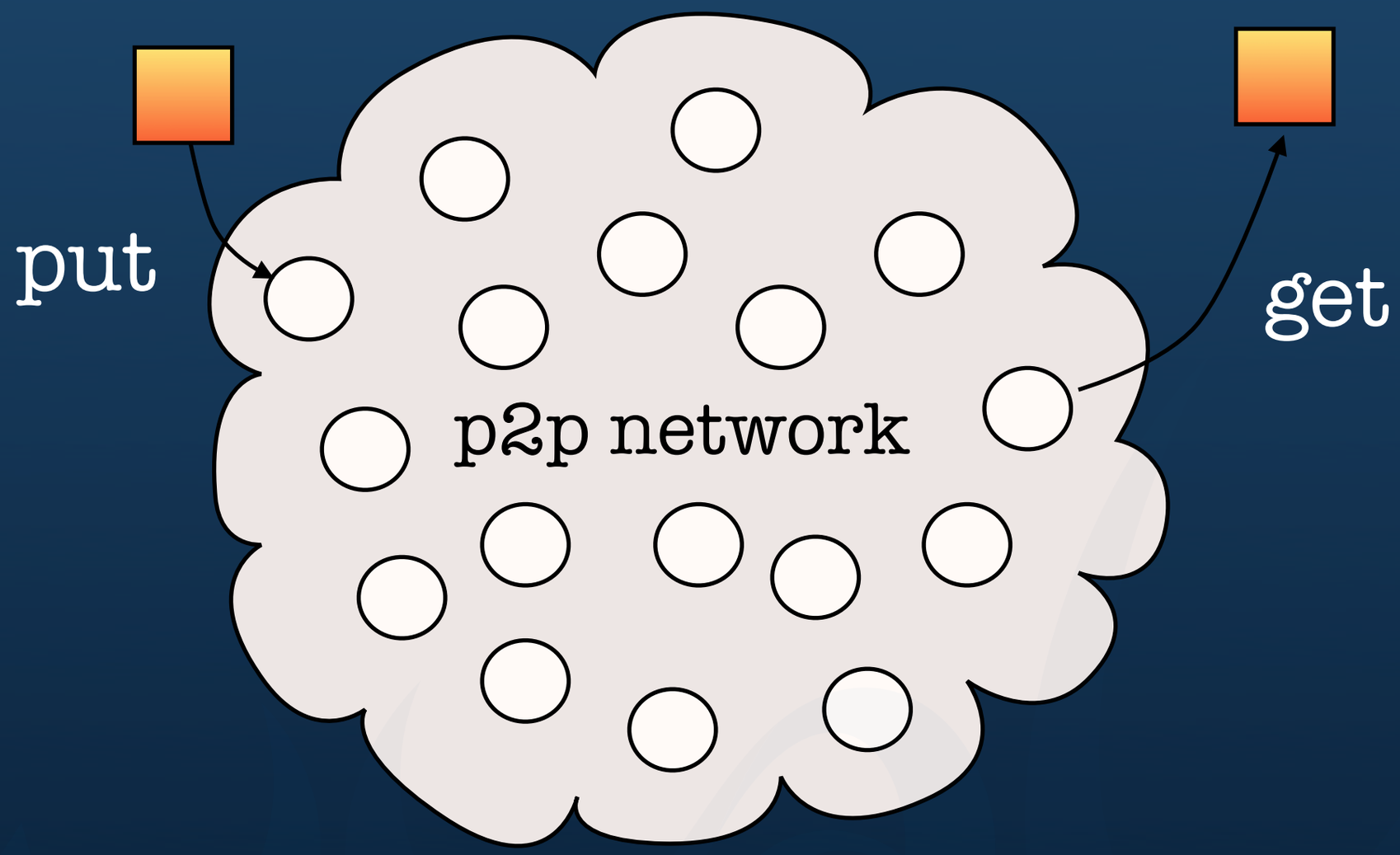


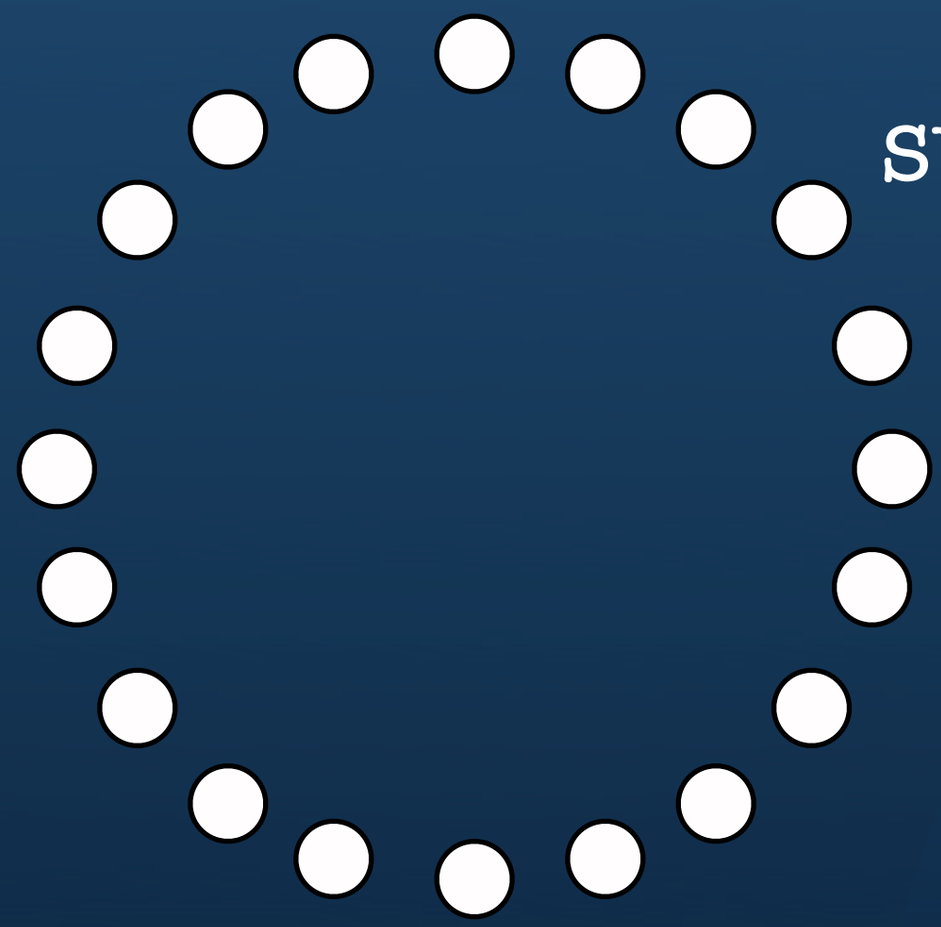

p2p network


put
p2p network

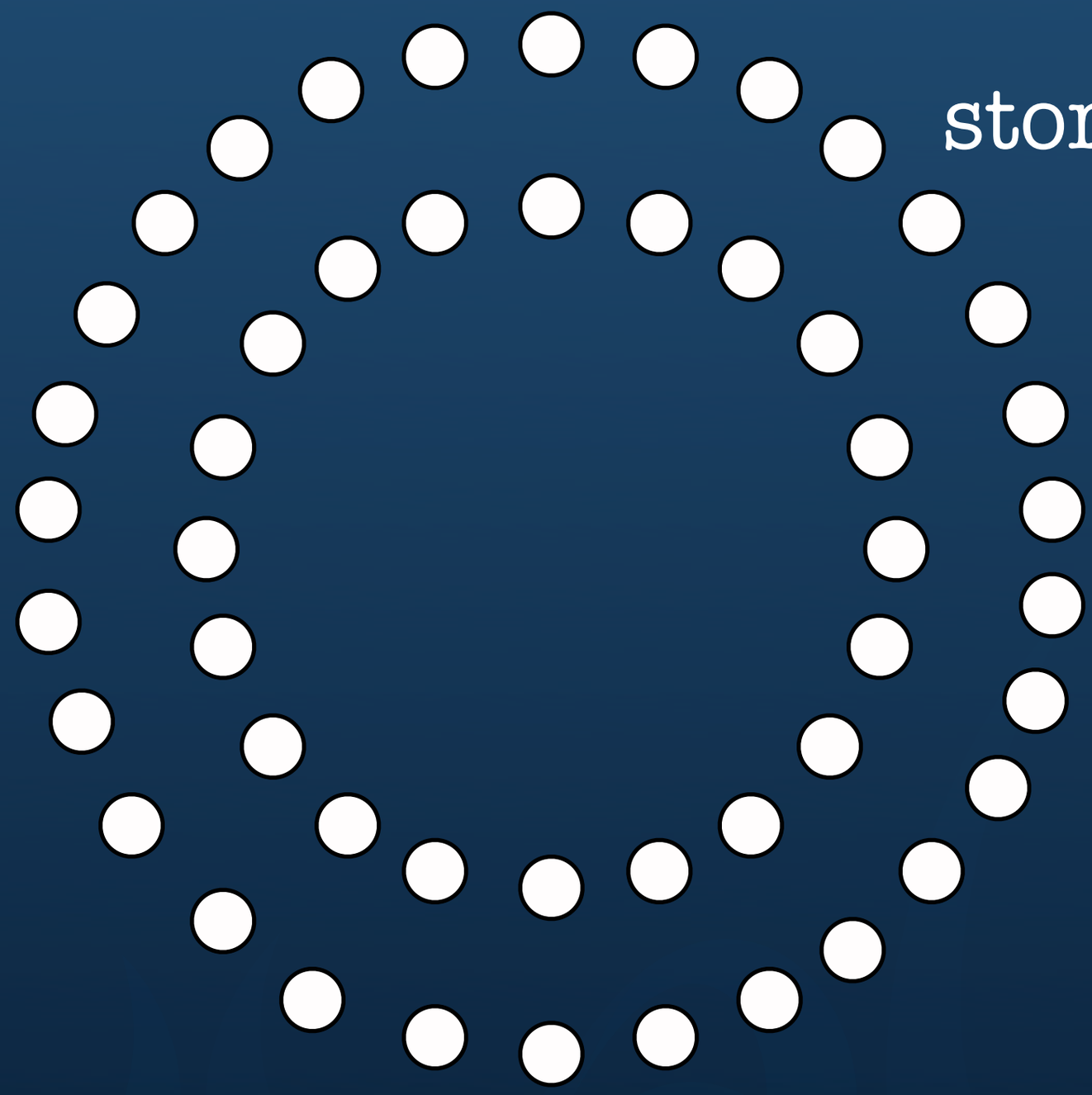

put
get
p2p network

distributed hash table (DHT)

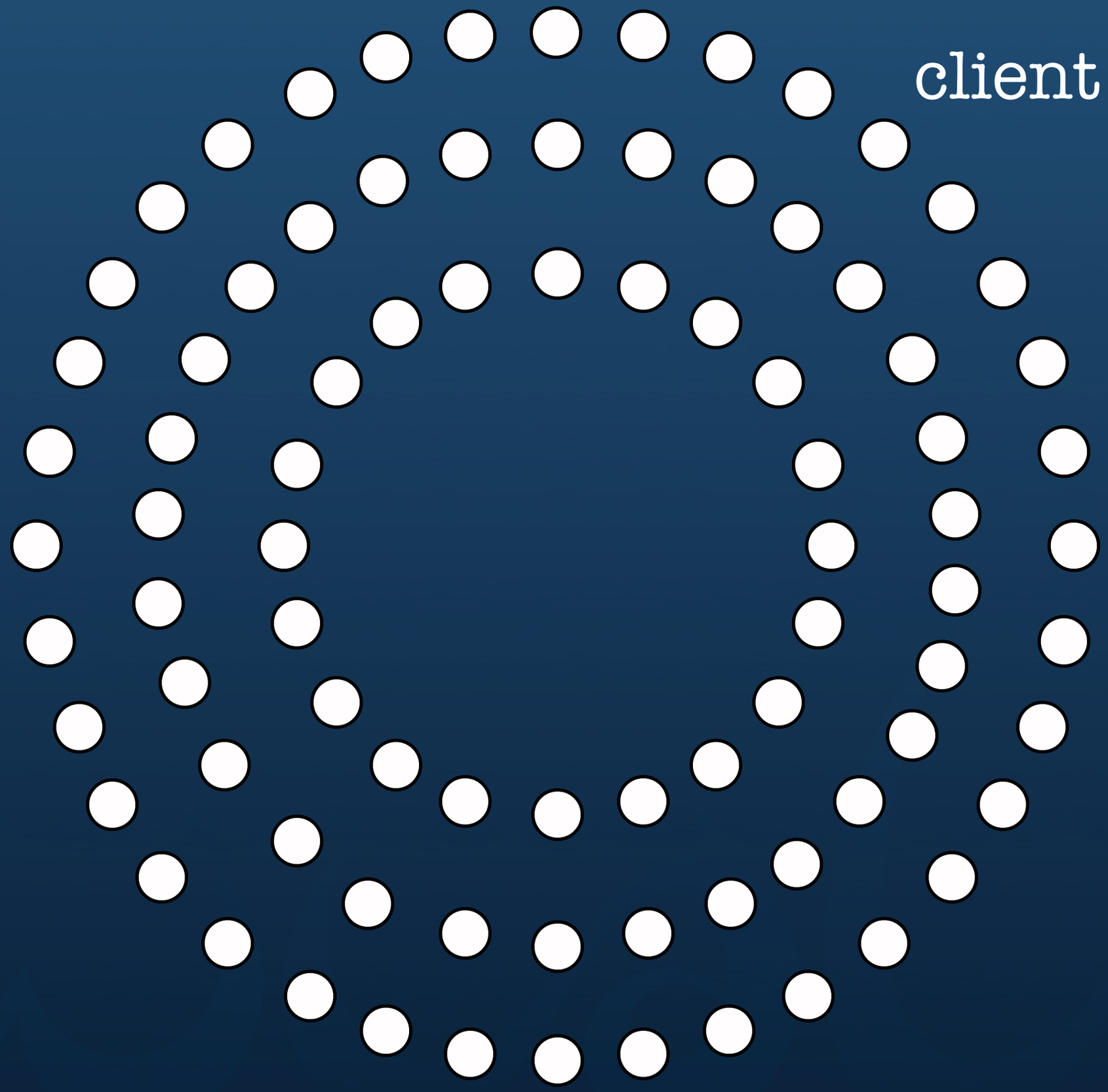


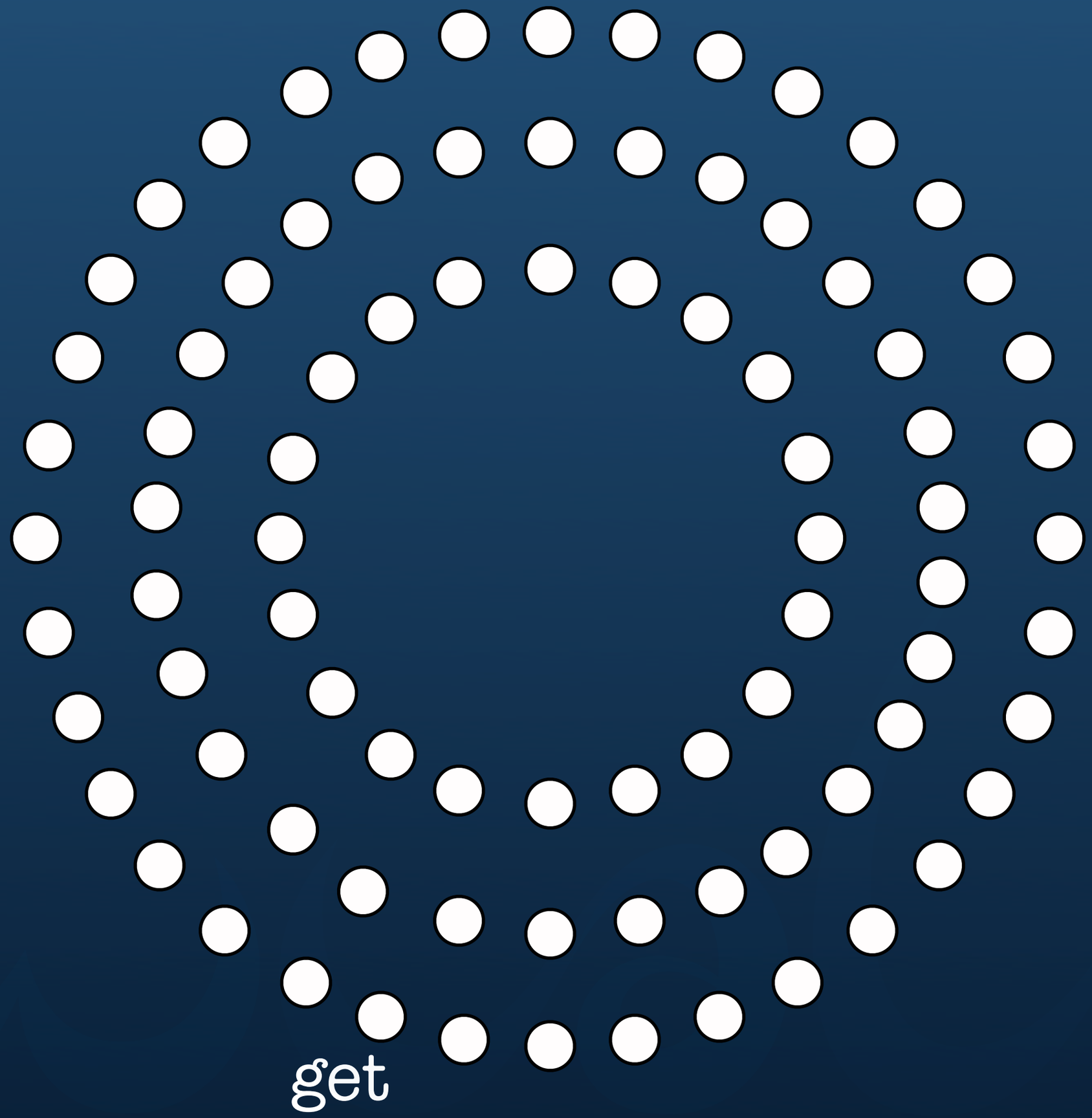


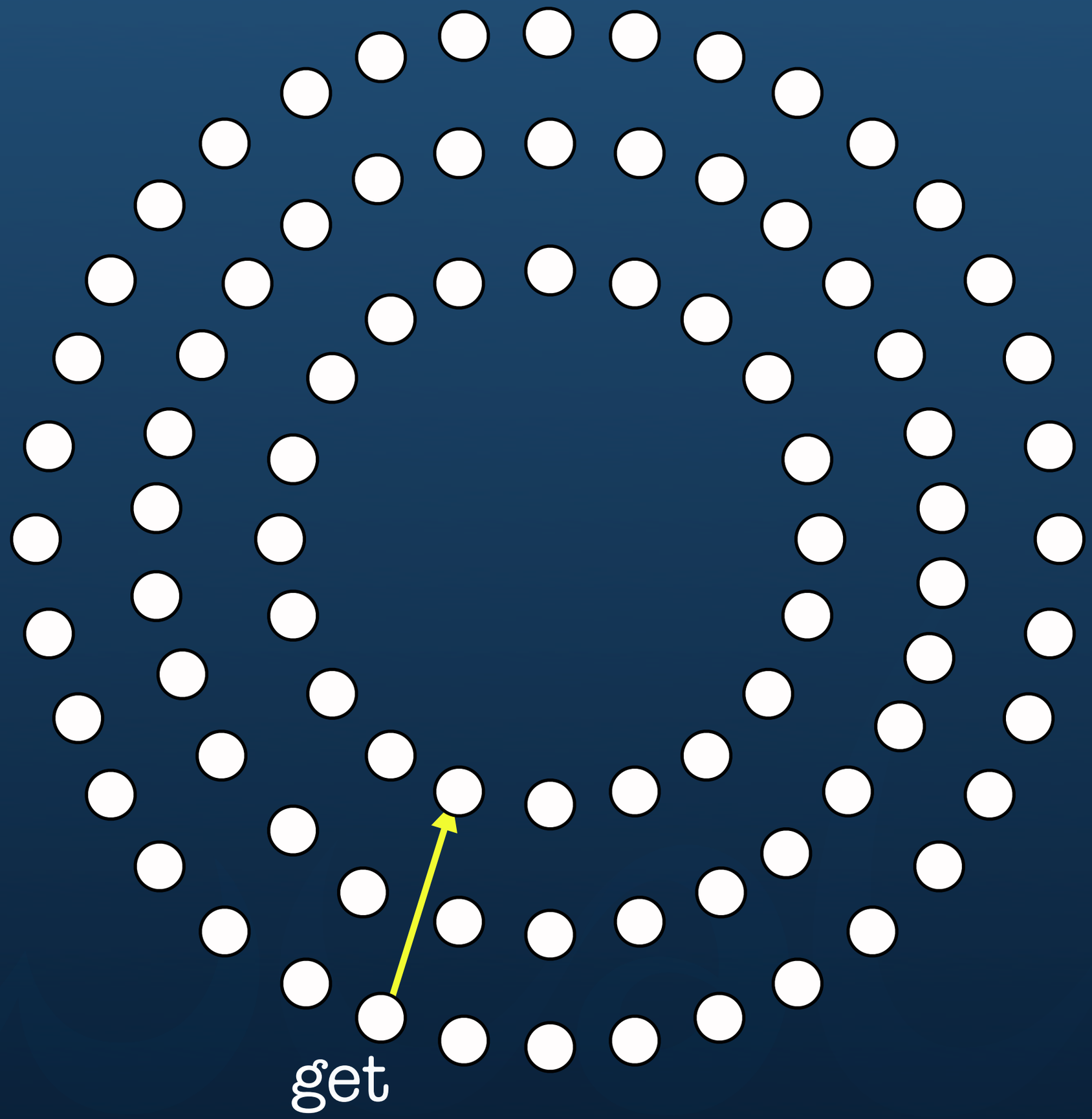
super nodes

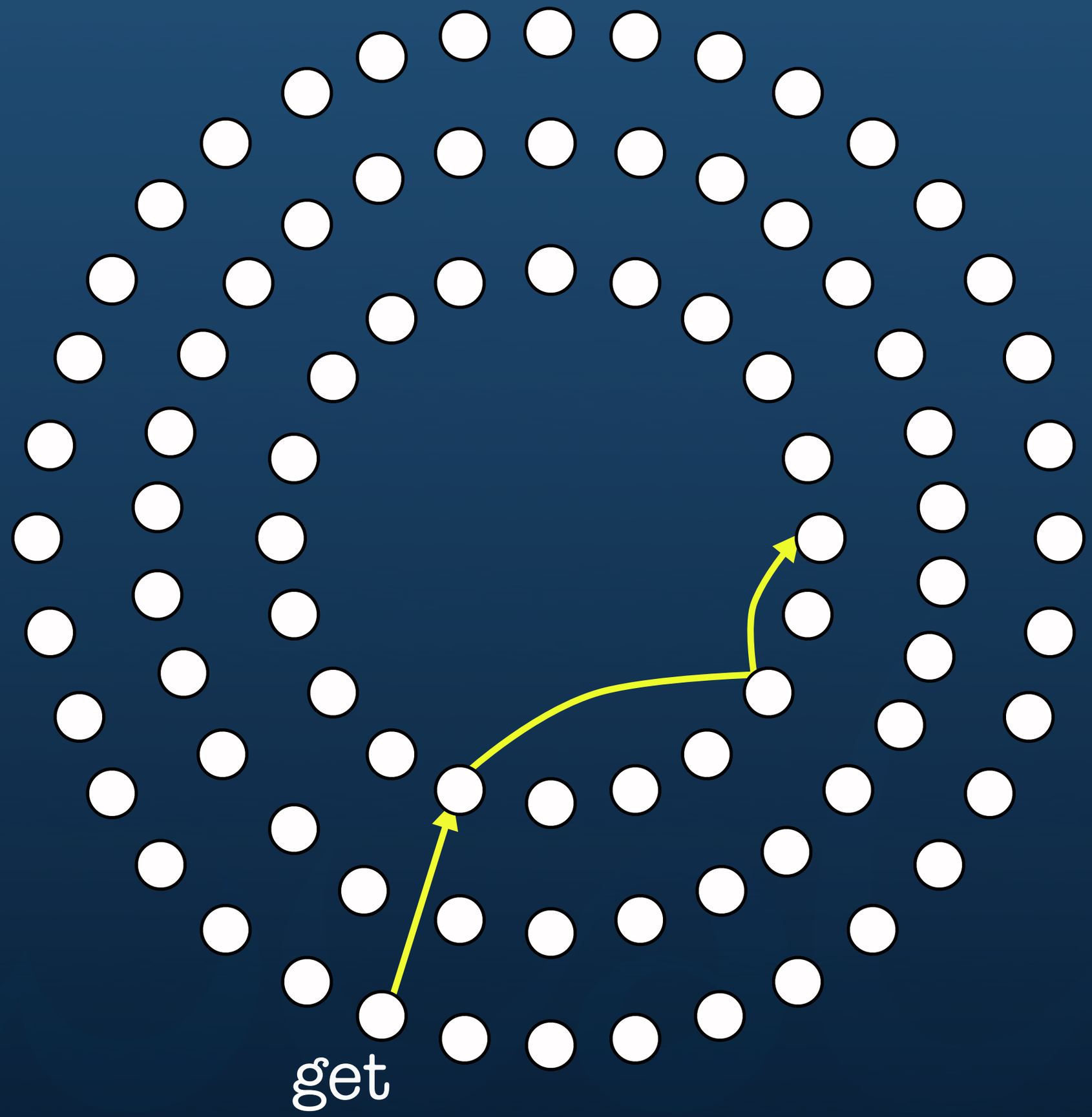


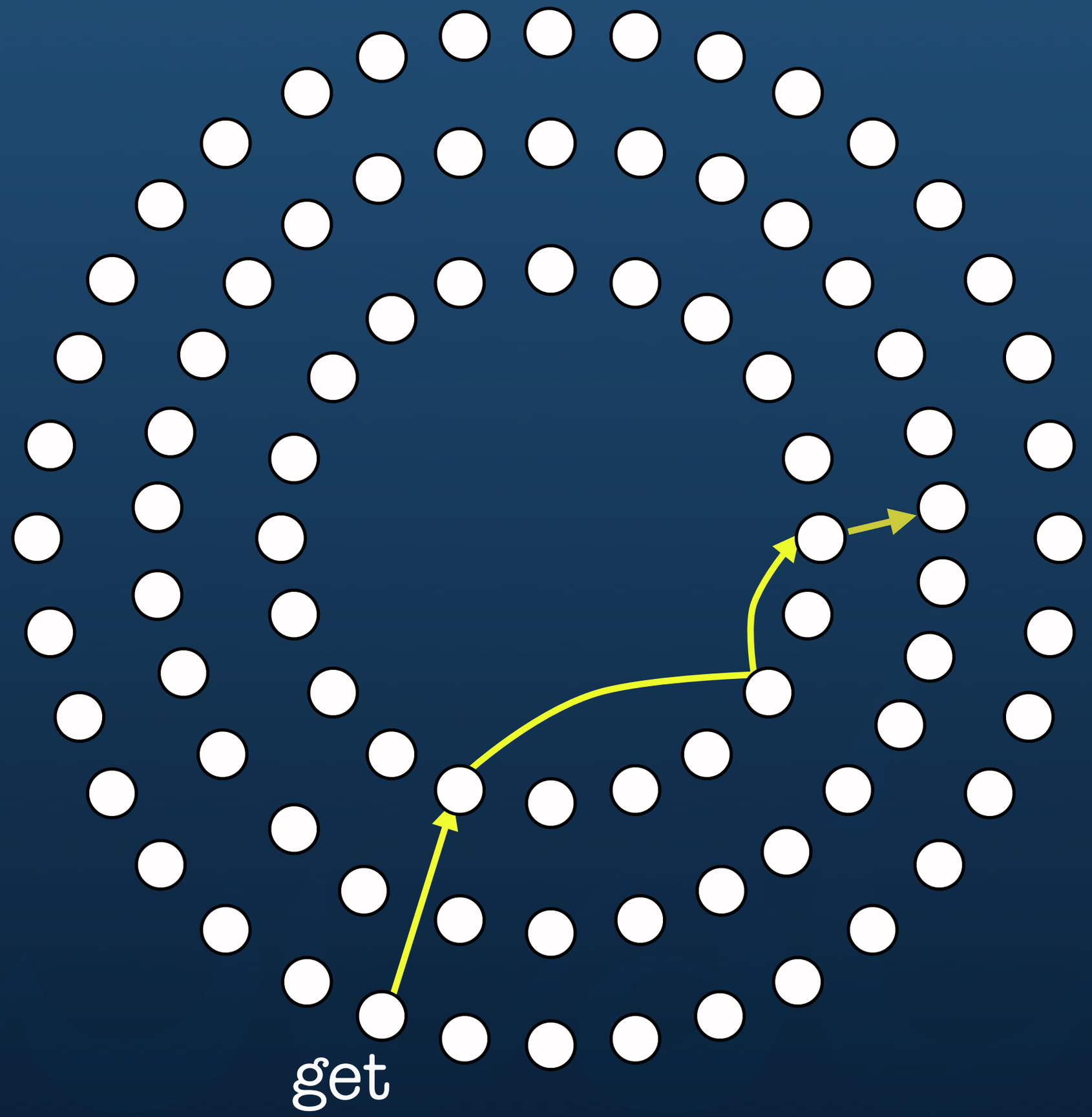
storage nodes

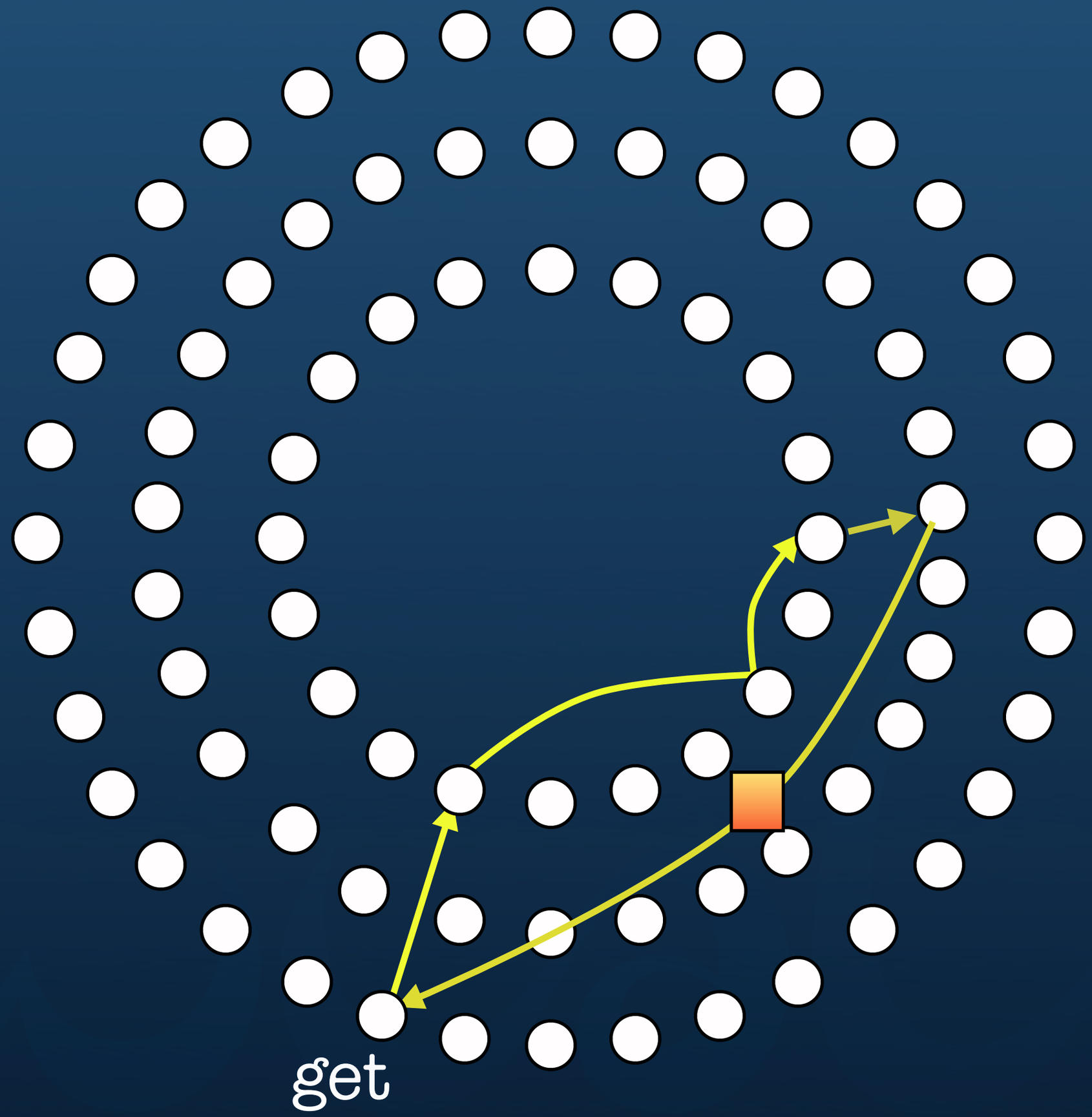

client nodes


get

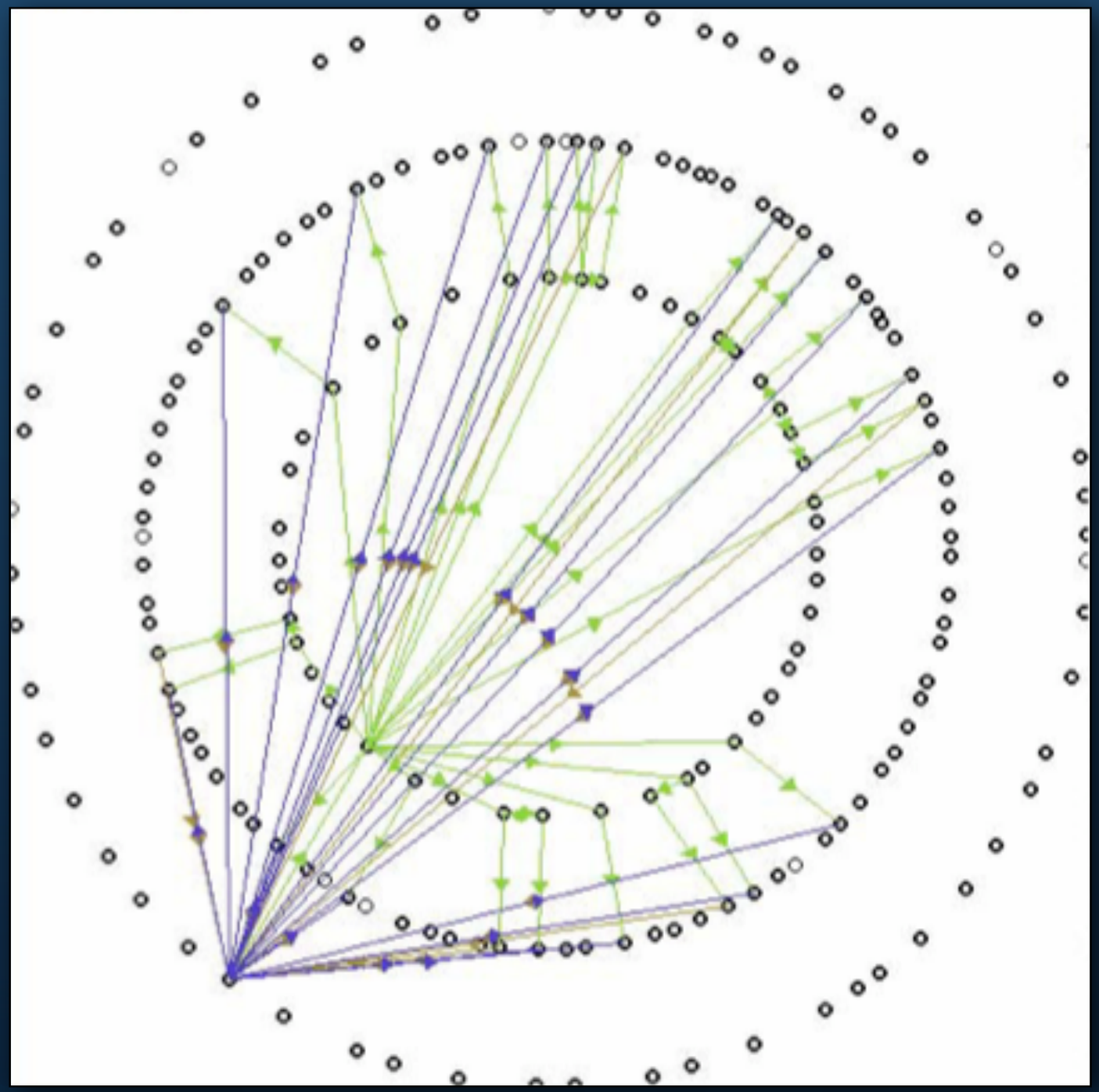

get


get


get


get

download of fragments (in parallel)



routing

napster: centralized :-(
gnutella: flooding :-(

chord, tapestry: structured overlay networks
O(log n) hops :-)
n = # super nodes

vulnerable to attacks (partitioning) :-(

super node
connected to direct neighbors
plus some random links

random links?
piggy-pack routing information

number of hops depends on

size of the network (n)

size of the routing table (R)

which itself depends on the traffic
we have lots of traffic due to erasure coding

simulation results

$n = 10^6$

$R = 1{,}000$: < 3 hops

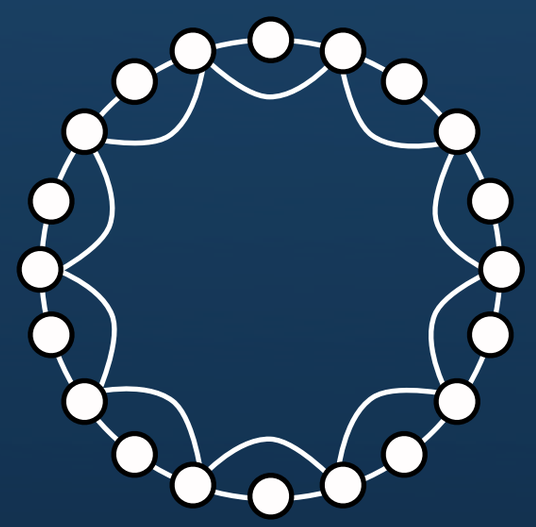
$R = 100$: ~5 hops

reasonable already with moderate traffic

small world effects

(see milgram, watts & strogatz, kleinberg)

regular graph

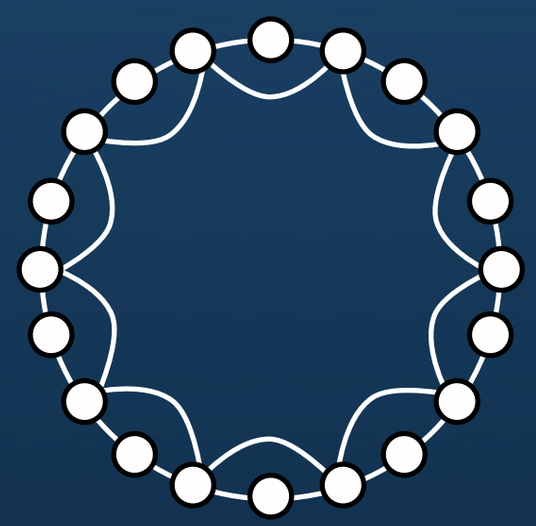


high diameter :-(
high clustering :-)

small world effects

(see milgram, watts & strogatz, kleinberg)

regular graph



high diameter :-(
high clustering :-)

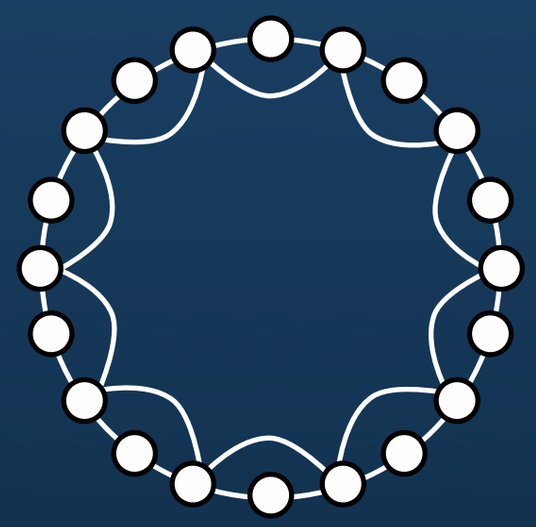
random graph

low diameter :-)
low clustering :-(

small world effects

(see milgram, watts & strogatz, kleinberg)

regular graph



high diameter :-(
high clustering :-)

random graph

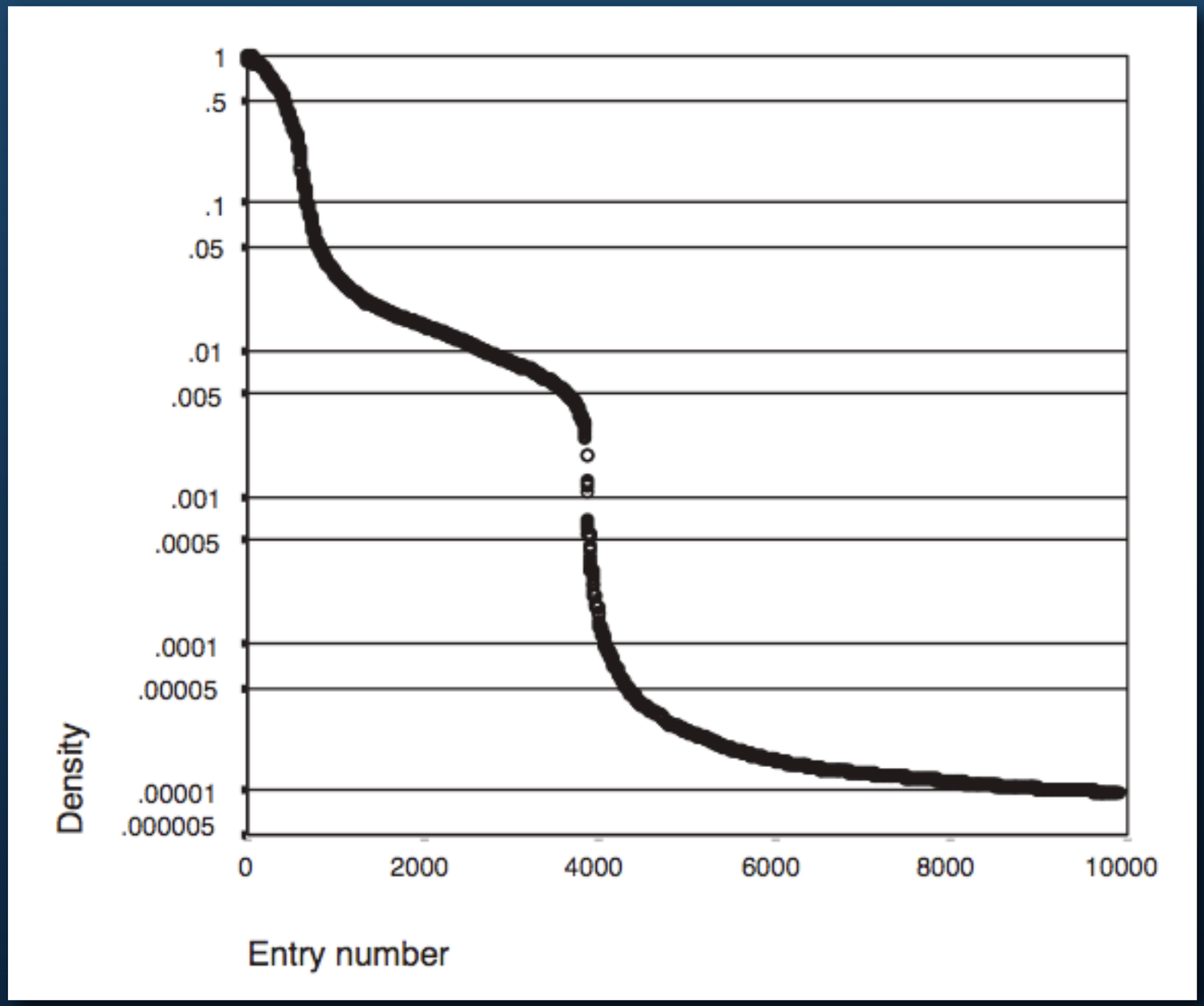
low diameter :-)
low clustering :-(

mix

low diameter :-)
high clustering :-)

routing table

$n = 10^9$, $R = 10{,}000$



incentives, fairness
prevent free-riding

local disk space
online time

upload bandwidth

online storage = local disk space * online time

example: 10 GB disk space, 70% online --> 7 GB

we have different mechanisms to measure
and check these two variables

trading storage

only if you want to (you start with 1 GB)

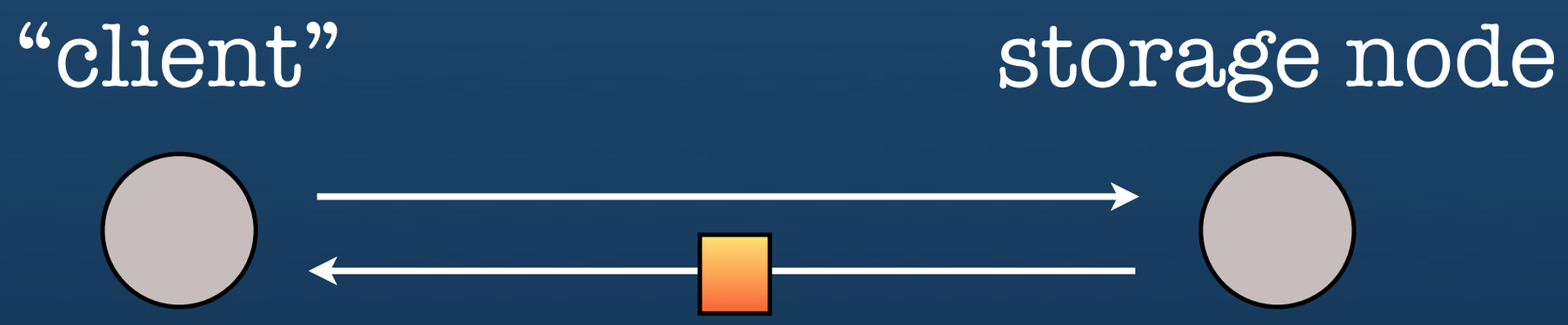
you must be online at least 17% of the time

(≈ 4 hours a day, running average)

storage can be earned on multiple computers

upload bandwidth

the more upload bandwidth you provide,
the more download bandwidth you get



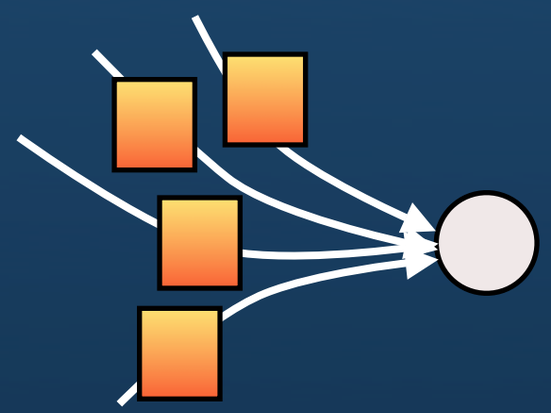
asymmetric interest
tit-for-tat doesn’t work :-(

believe the software? hack it (kazaa lite) :-(

distributed reputation system
that is not susceptible to false reports
and other forms of cheating

must scale well with number of transactions
we have lots of small transactions due to erasure coding

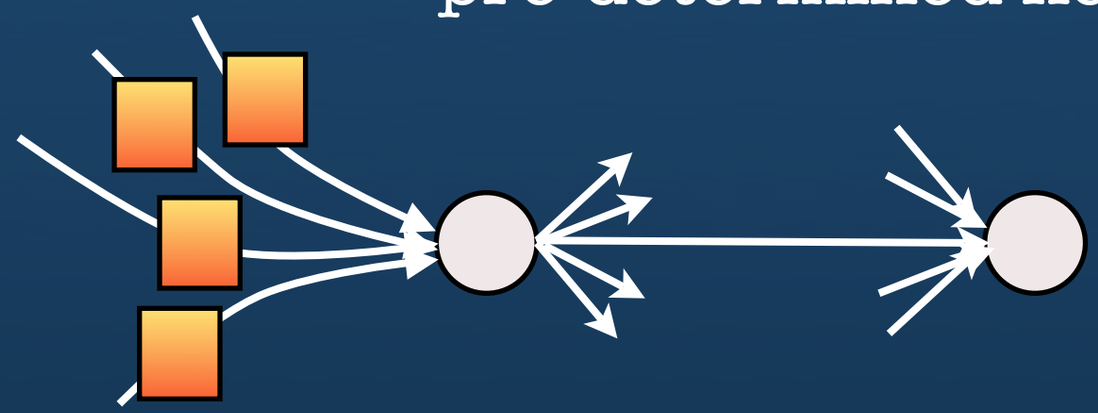
Havelaar, NetEcon 2006



1. lots of transactions
   "observations"

Havelaar, NetEcon 2006

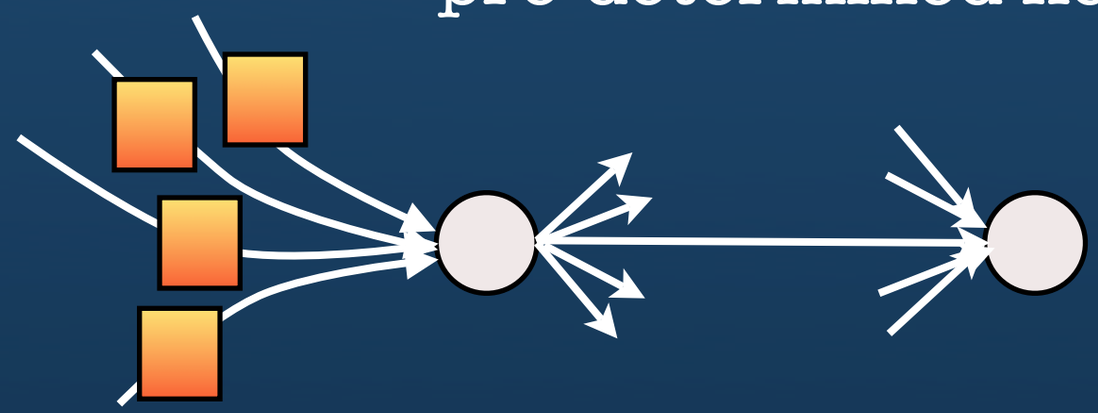
2. every round (e.g., a week)
send observations to
pre-determined neighbors (hash code)



1. lots of transactions
"observations"

Havelaar, NetEcon 2006

2. every round (e.g., a week)
send observations to
pre-determined neighbors (hash code)

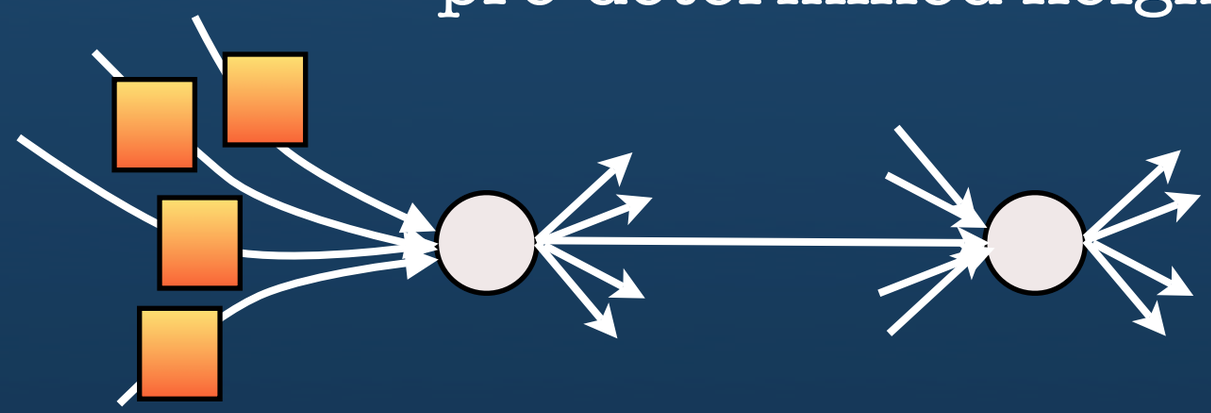


3. discard ego-reports,
median, etc.

1. lots of transactions
"observations"

Havelaar, NetEcon 2006

2. every round (e.g., a week)
send observations to
pre-determined neighbors (hash code)



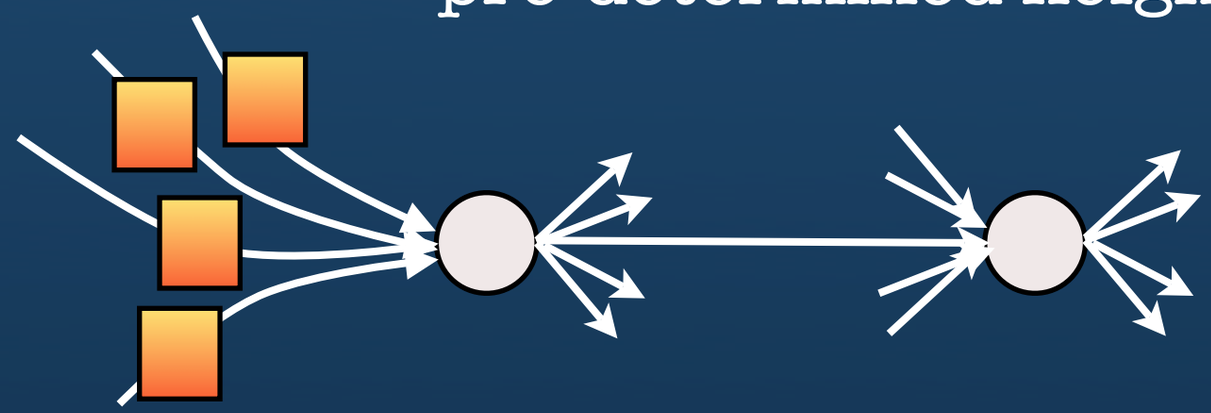
3. discard ego-reports,
median, etc.

4. next round, aggregate

1. lots of transactions
"observations"

Havelaar, NetEcon 2006

2. every round (e.g., a week)
send observations to
pre-determined neighbors (hash code)



3. discard ego-reports,
median, etc.

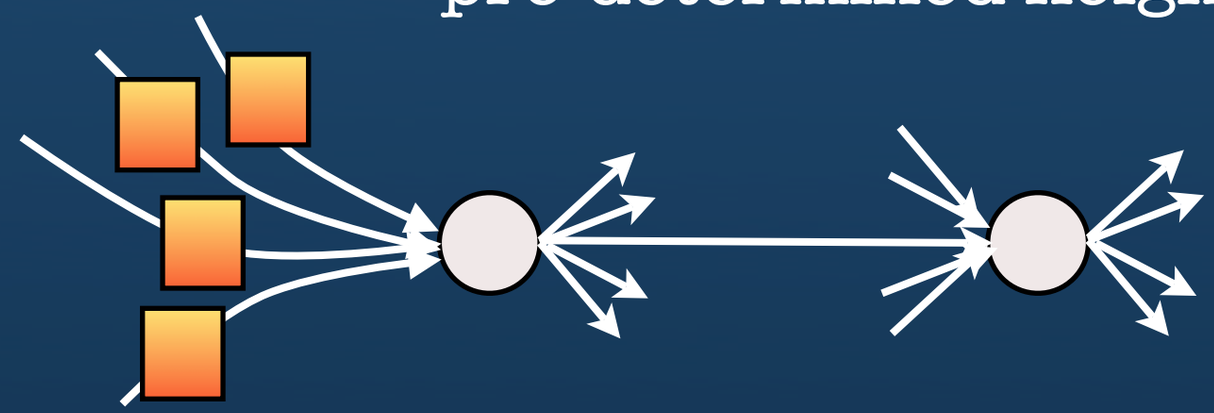
4. next round, aggregate

1. lots of transactions
“observations”

5. update reputation
of storage nodes

Havelaar, NetEcon 2006

2. every round (e.g., a week)
send observations to
pre-determined neighbors (hash code)



3. discard ego-reports,
median, etc.

4. next round, aggregate

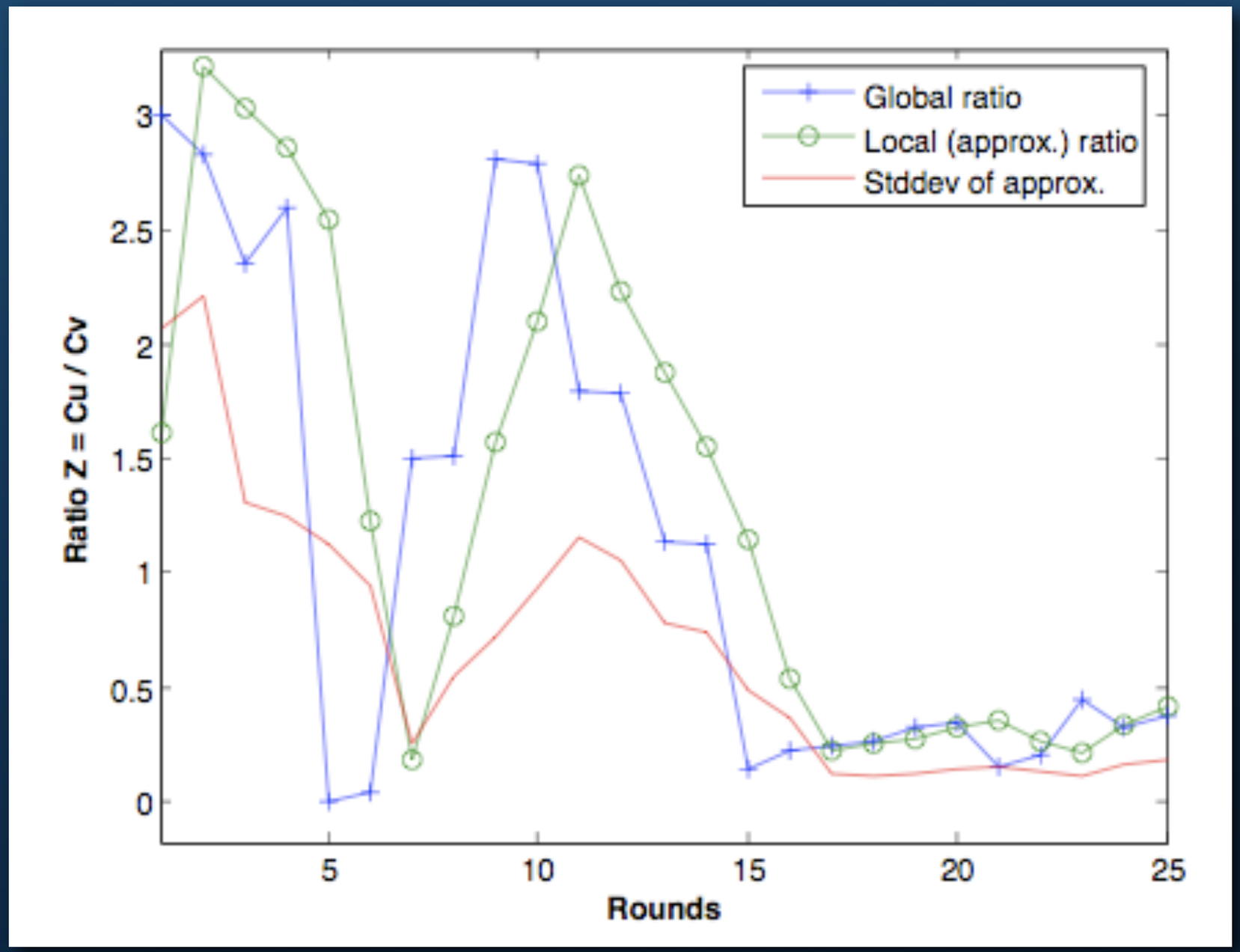
1. lots of transactions
"observations"

5. update reputation
of storage nodes

rewarding:
upload bandwidth
proportional
to reputation

Havelaar, NetEcon 2006

local approximation of contribution

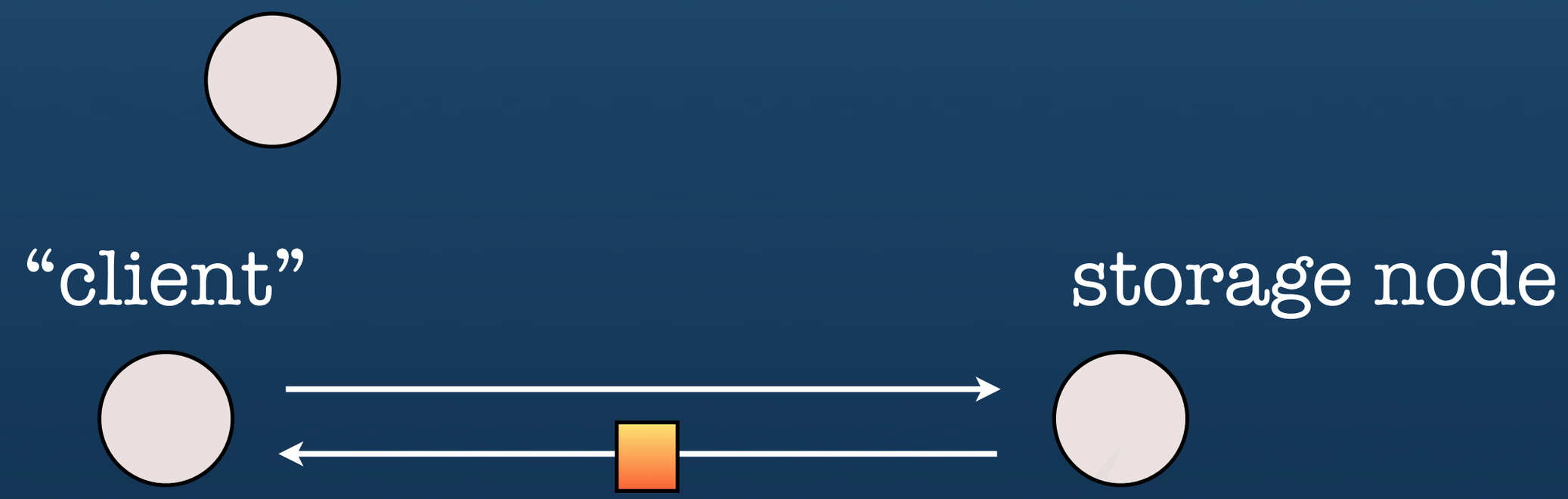


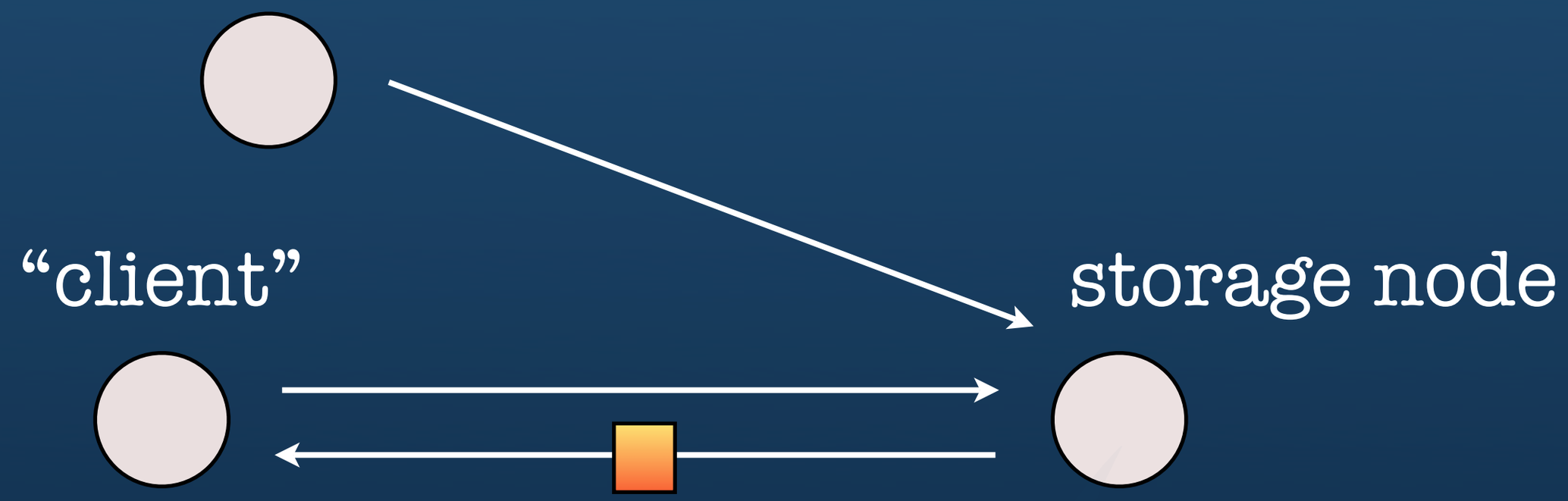
Havelaar, NetEcon 2006

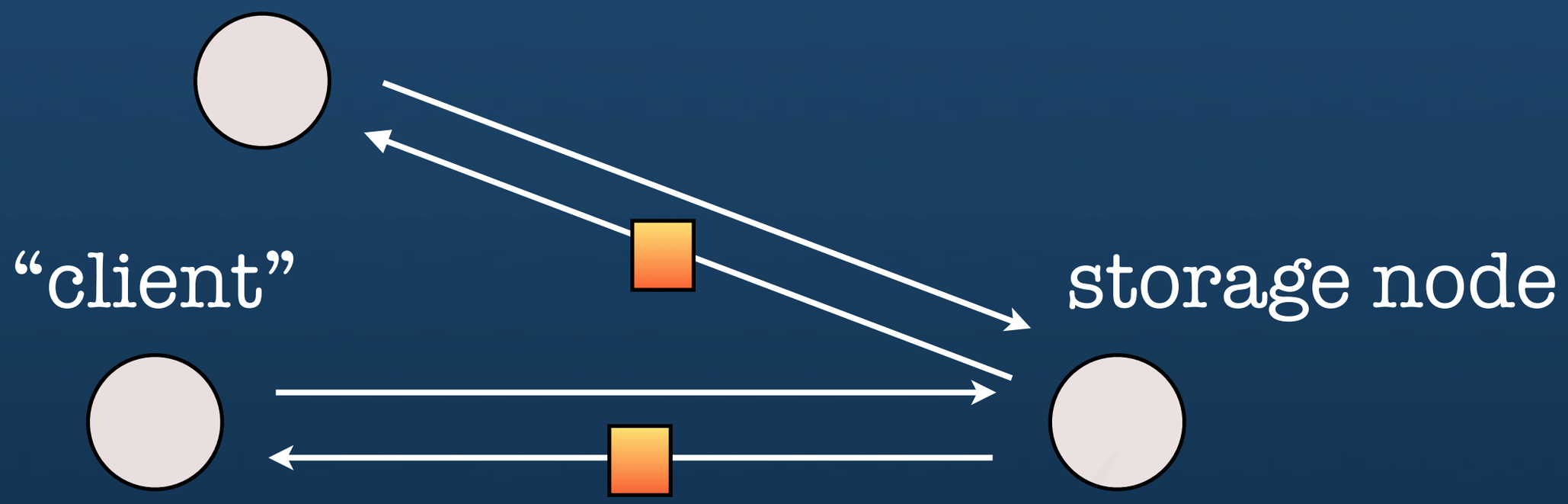
“client”
storage node

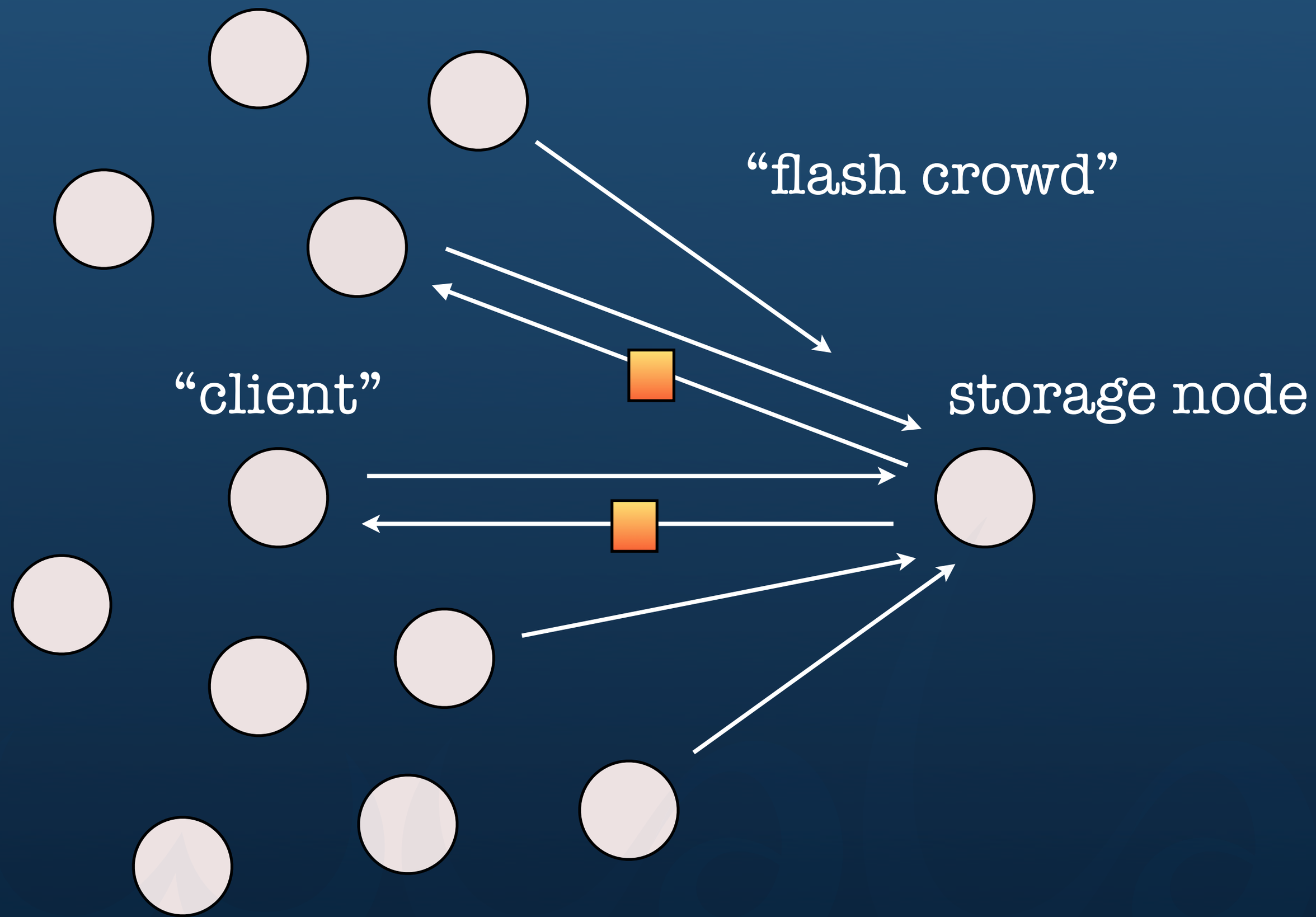
“client”
storage node

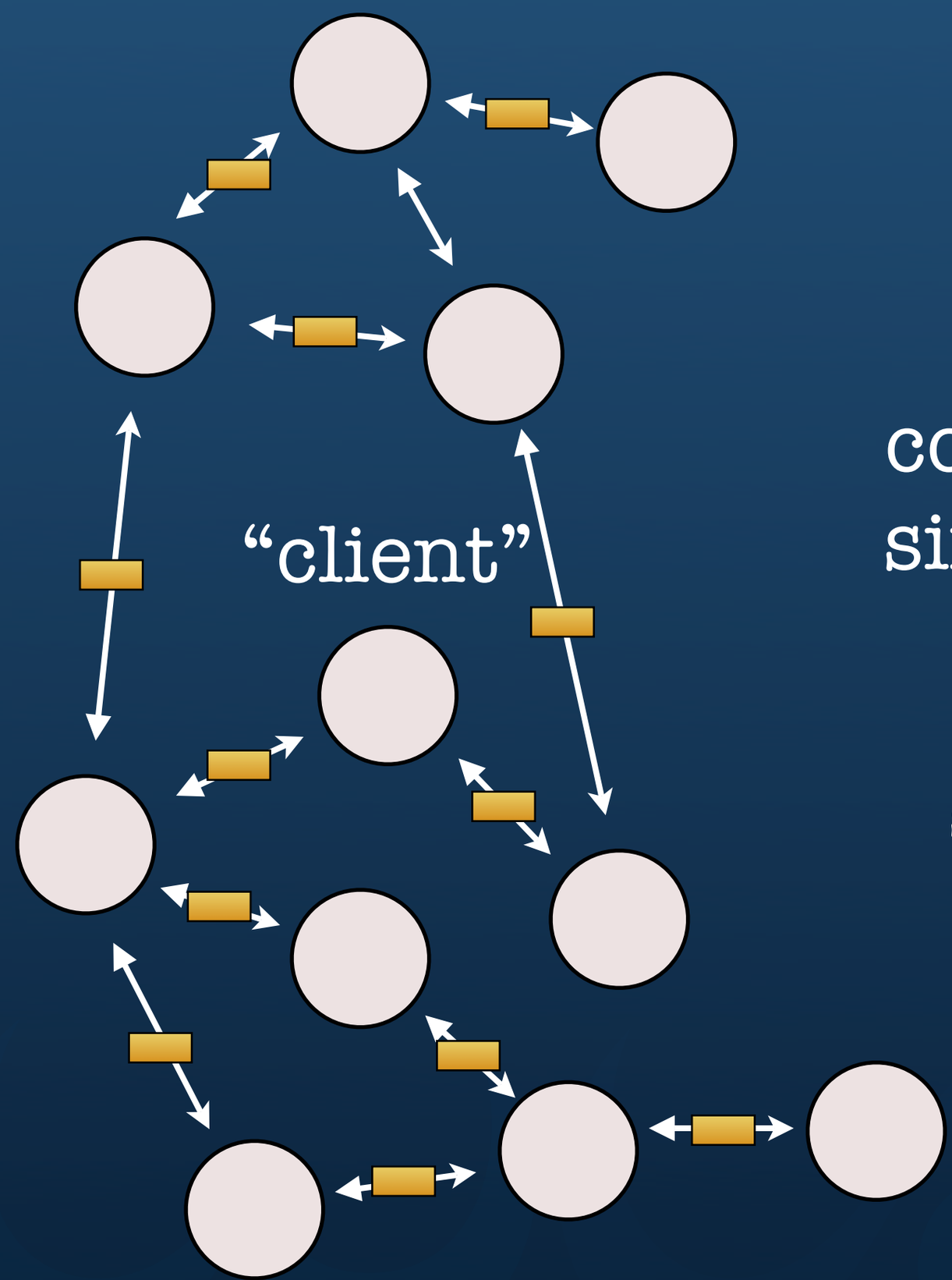
“client”
storage node


“client”
storage node


"client"
storage node


"client"
storage node


"flash crowd"
"client"
storage node



content distribution
similar to bittorrent
tit-for-tat

some differences due to
erasure codes

encryption

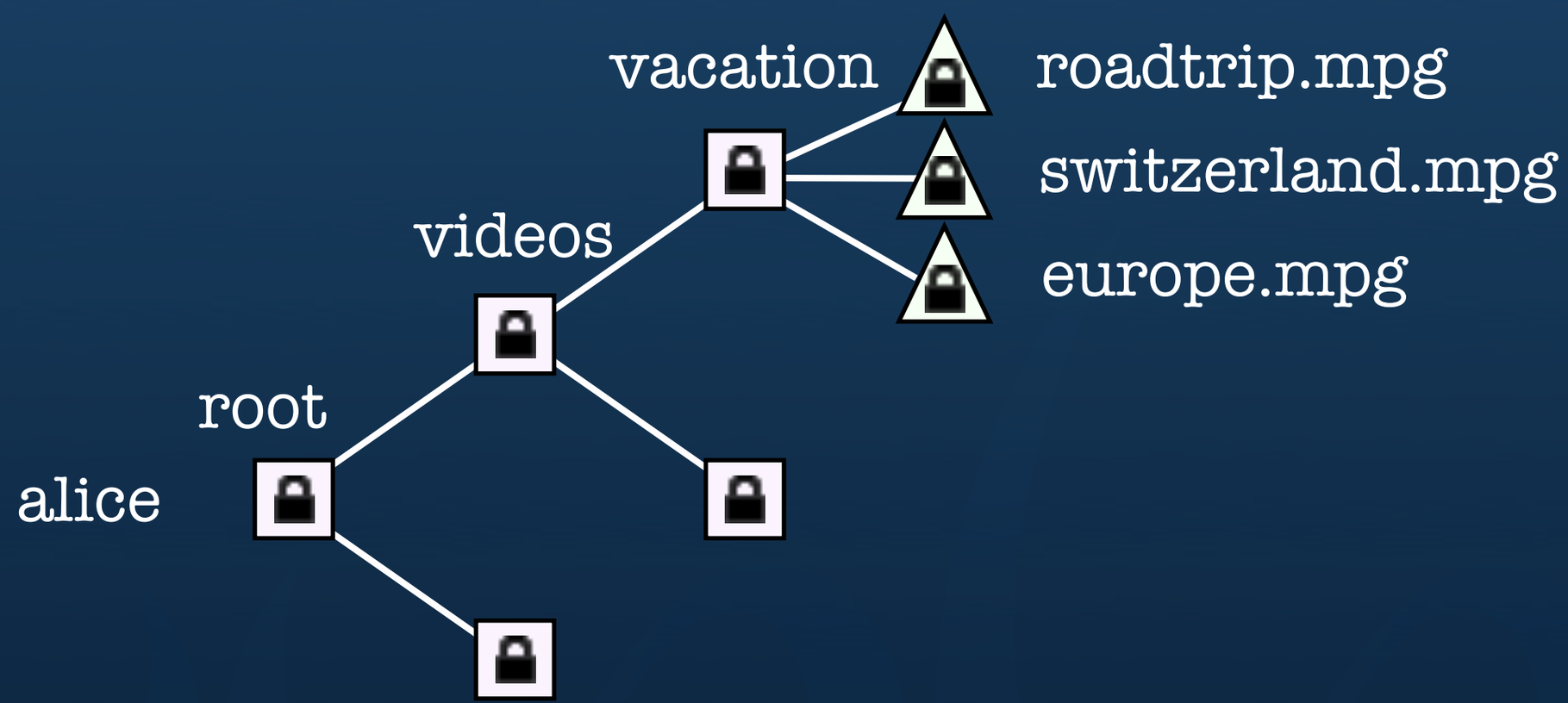
128 bit AES for encryption
2048 bit RSA for authentication

all data is encrypted (file + meta data)
all cryptographic operations performed locally
(i.e., on your computer)

access control

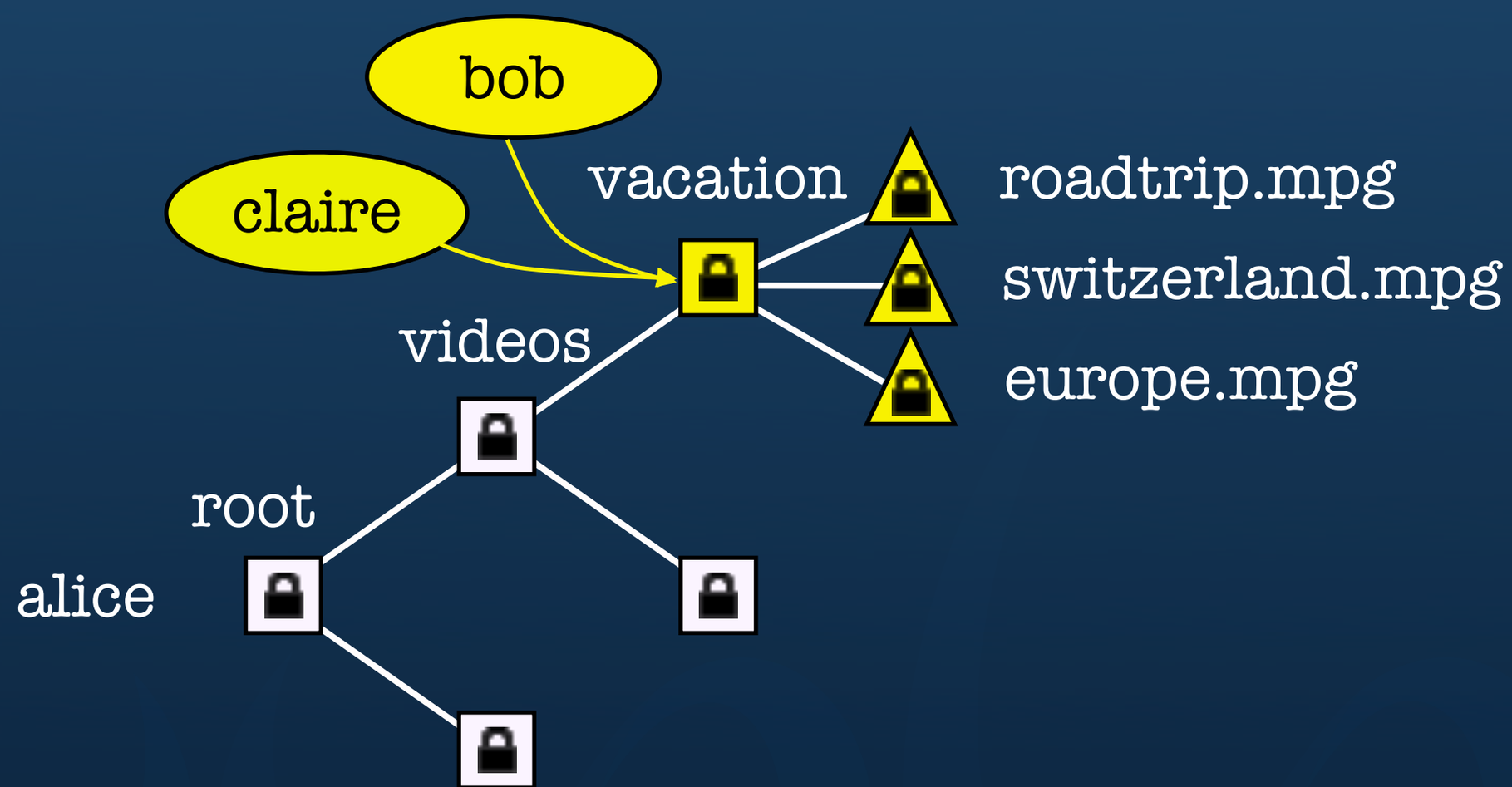
cryptographic tree structure
untrusted storage
doesn't reveal who has access
very efficient for typical operations
(grant access, move, etc.)

Cryptree, SRDS 2006



Cryptree, SRDS 2006

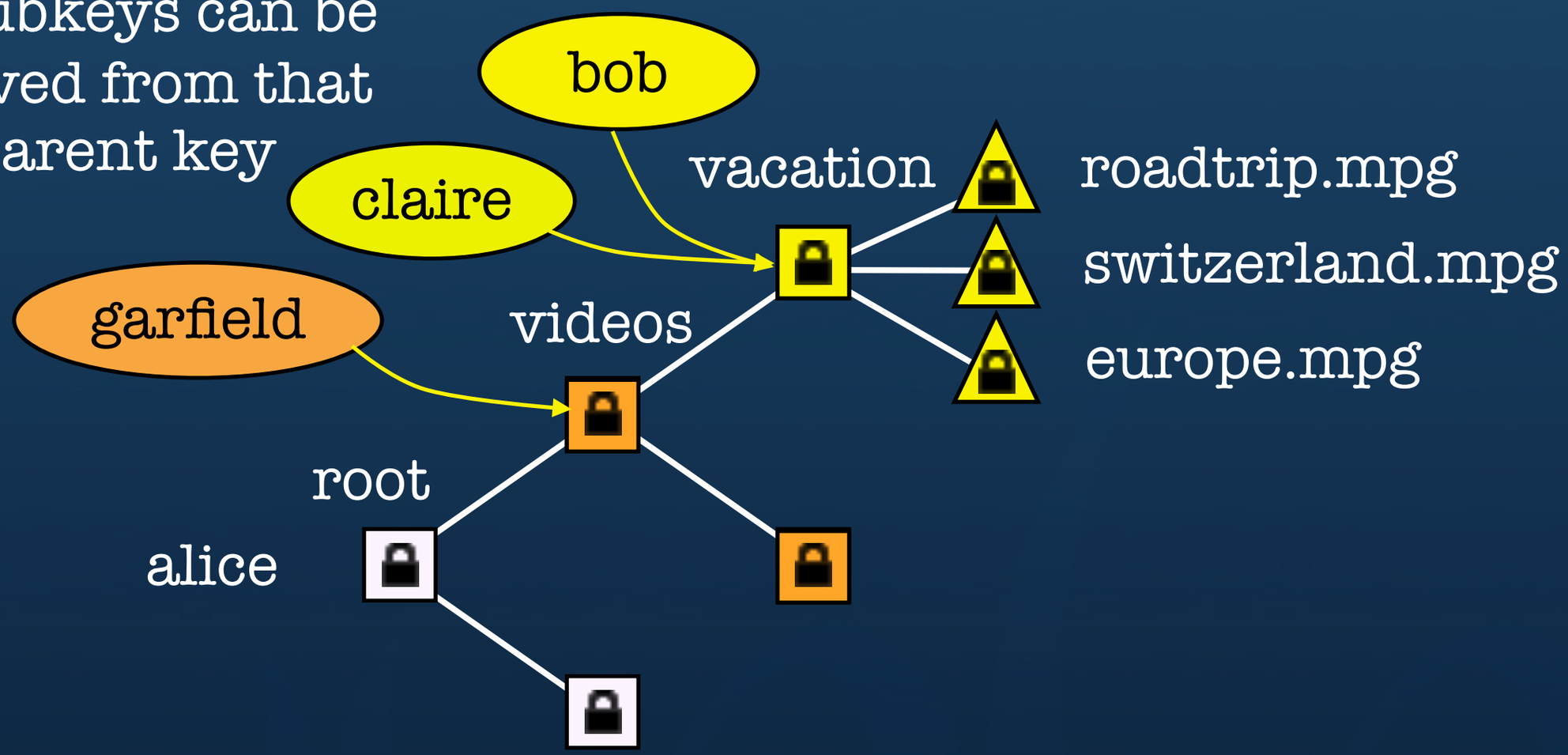
bob doesn't see that
claire has also access
and vice versa



Cryptree, SRDS 2006

granting access to this and all subfolders takes just one operation all subkeys can be derived from that parent key

bob doesn't see that claire has also access and vice versa



Cryptree, SRDS 2006

Thank you!

Questions?