Intro to Decentralized Systems

Nicola Greco

Protocol Labs

disclaimer

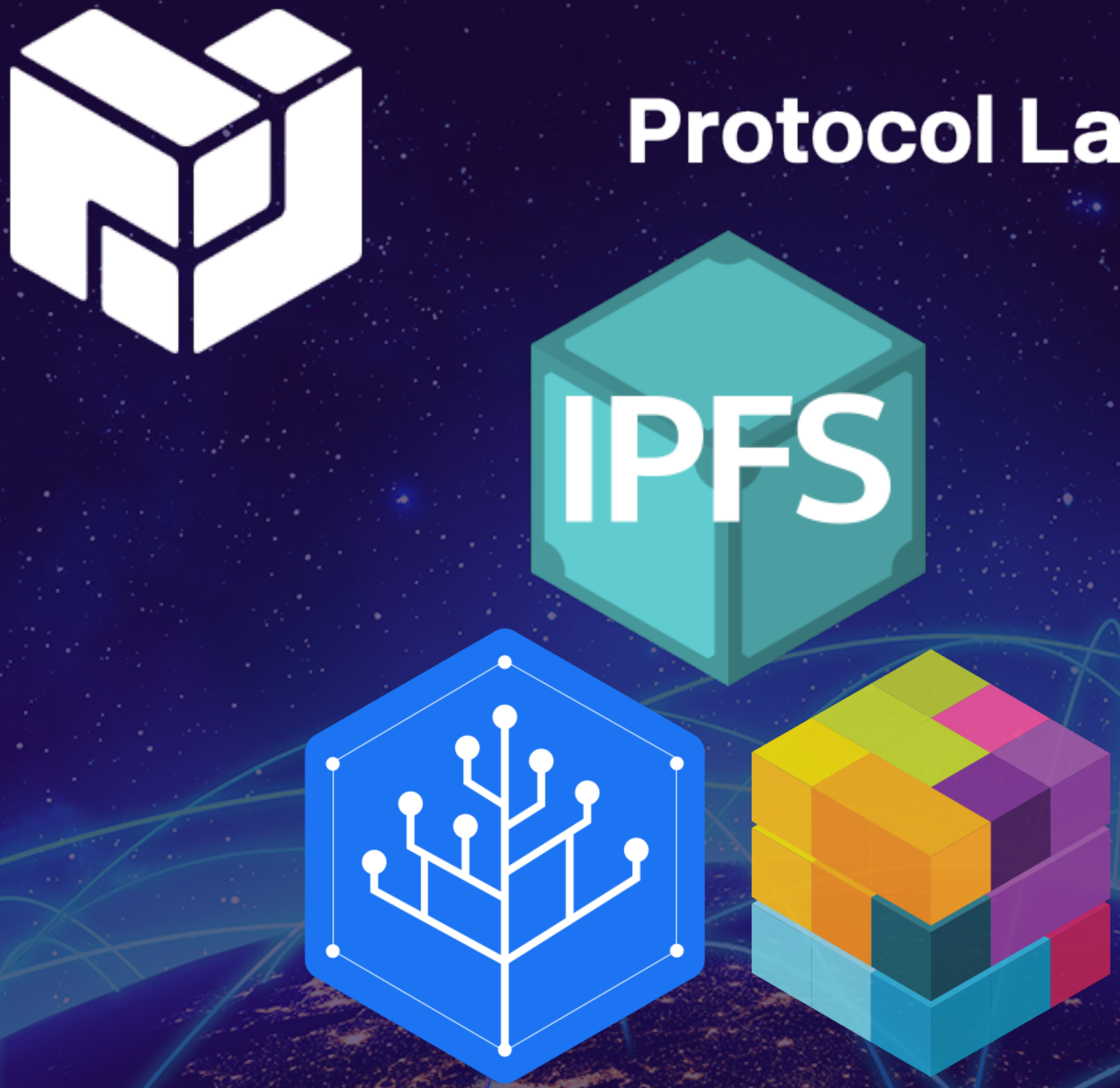
Protocol Labs

Protocol Labs

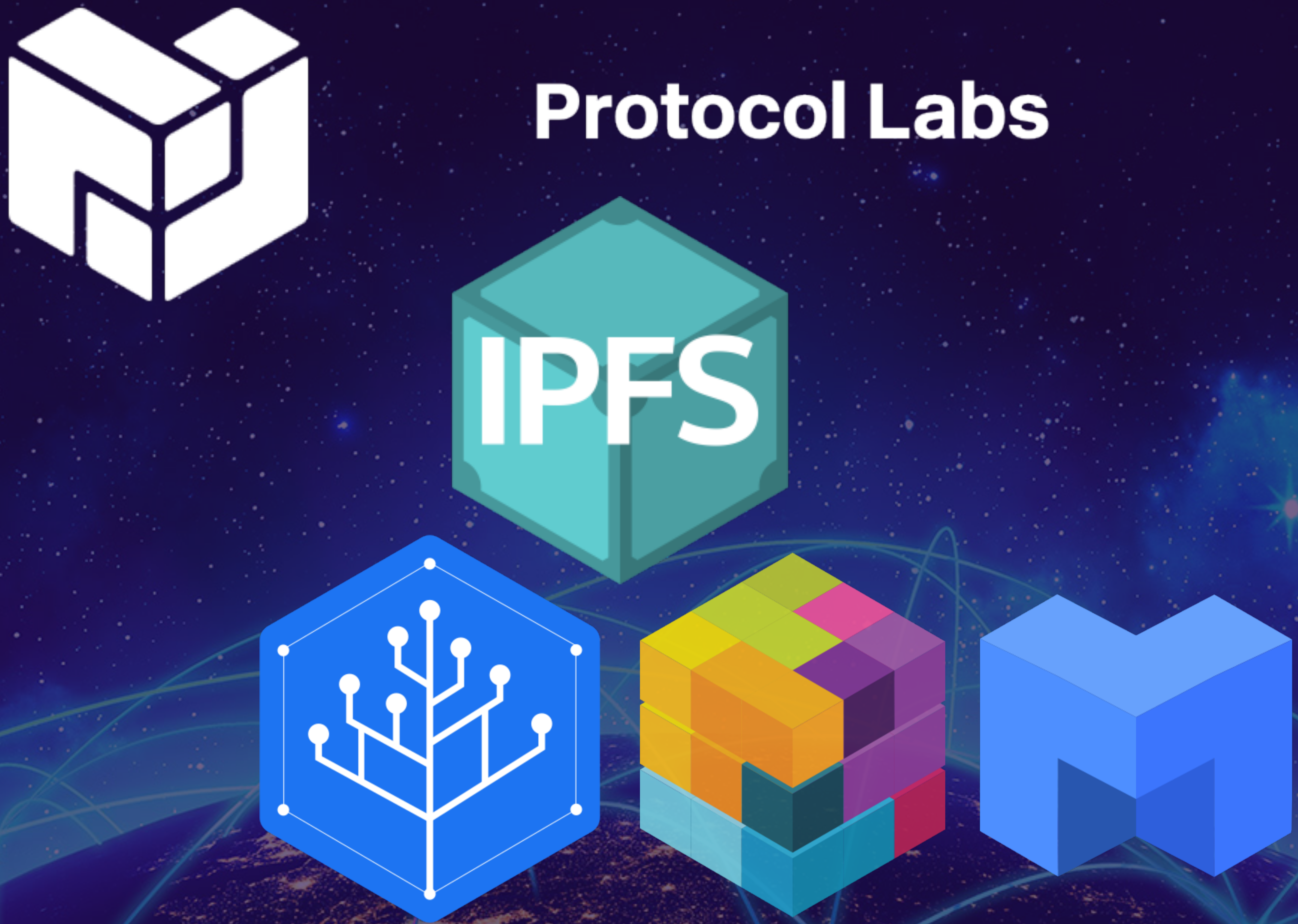
IPFS

Protocol Labs

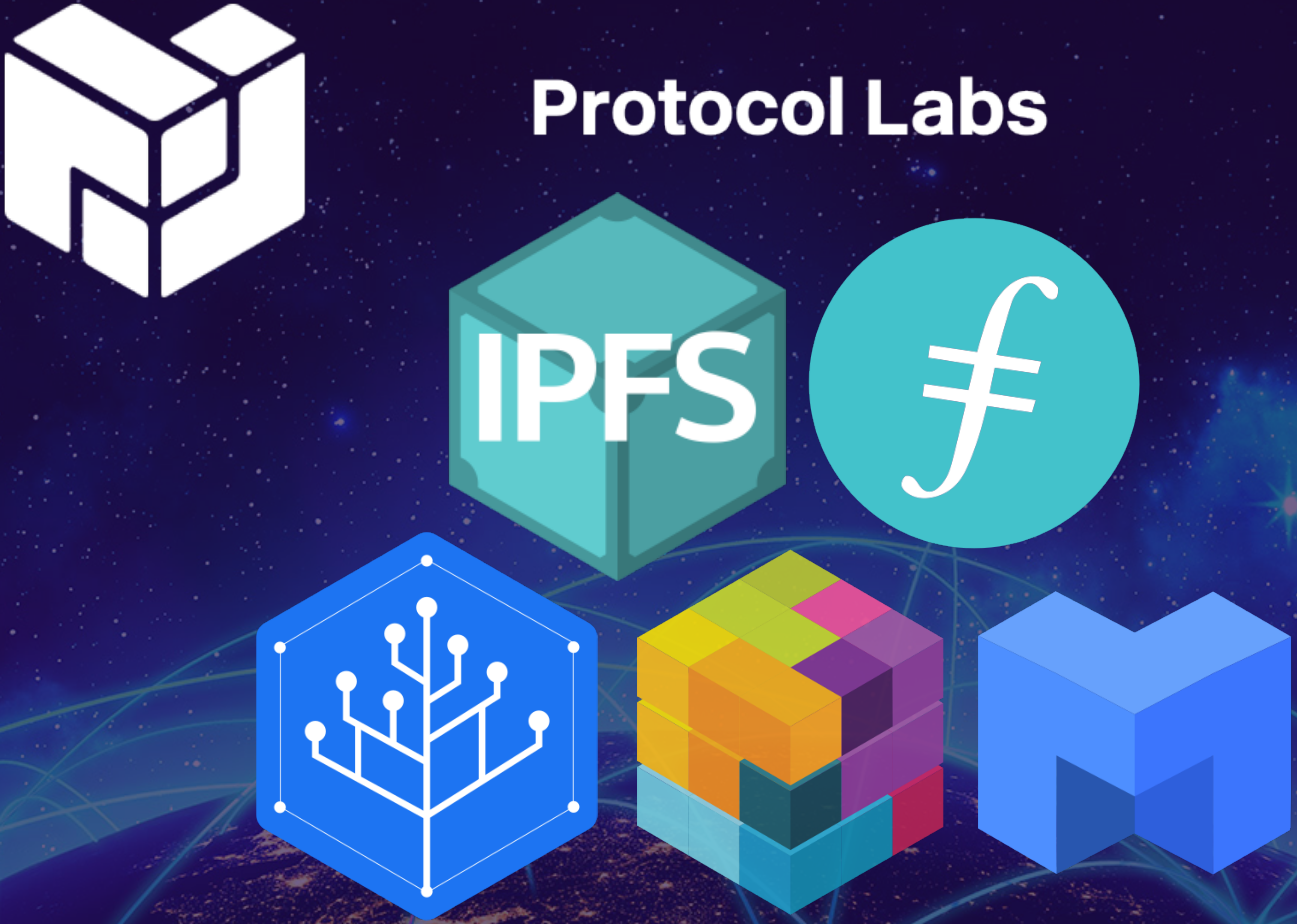
Protocol Labs



Protocol Labs



Protocol Labs



Part 1 Decentralized Web
Part 2 Universal Services
Part 3 Decentralized Storage
Part 4 Cryptonetworks

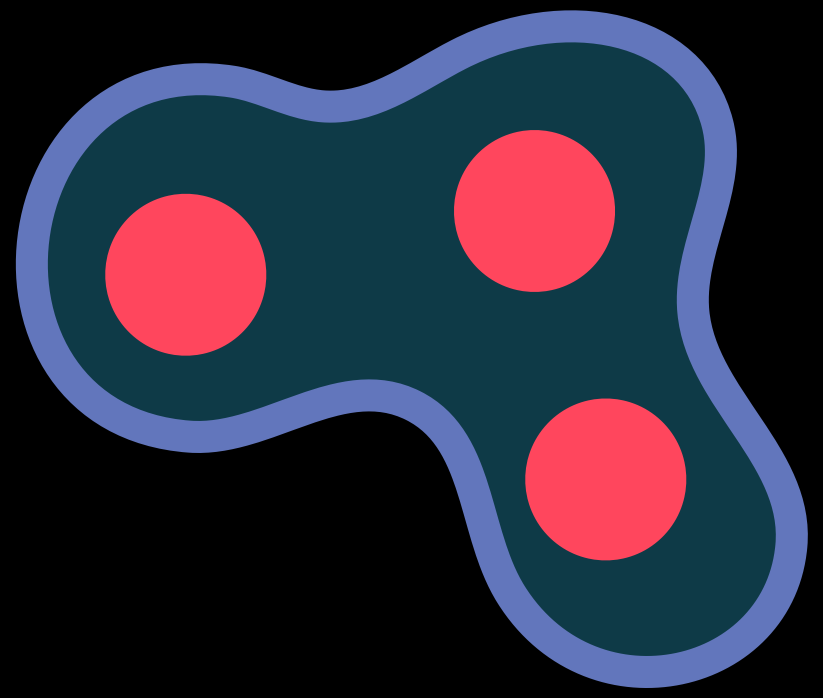
Part 1

Decentralizing the Web

decentralization = de-concentration of power

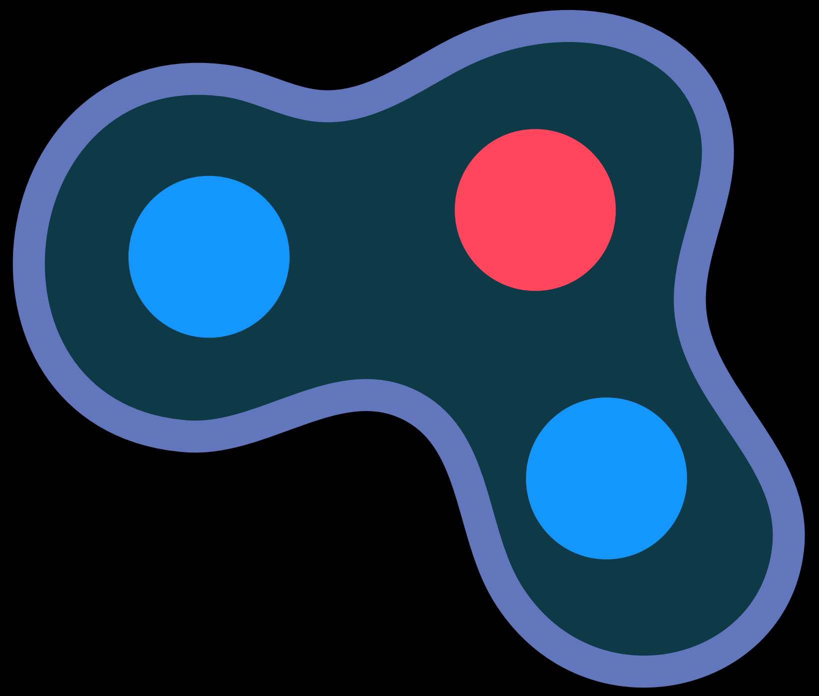
Benkler 2016

distributed system



decentralized system

no single authority fully trusted



minimize risk from misbehaving nodes

Web

Server <> Client

Server provides the right service

Server uses data responsibly

Server is secure

Server is always online

Server is single point of reference

Web

Server <> Client

Server provides the right service
Server uses data responsibly
Server is secure
Server is always online
Server is single point of reference

P2P

Server <> Server

Altruistic Network
Peers are equal

Web

Server <> Client

Server provides the right service

Server uses data responsibly

Server is secure

Server is always online

Server is single point of reference

P2P

Server <> Server

Altruistic Network

Peers are equal

Incentivized Protocols

Network <> Client

Clients delegate their service to the network

The network is “paid” to do so

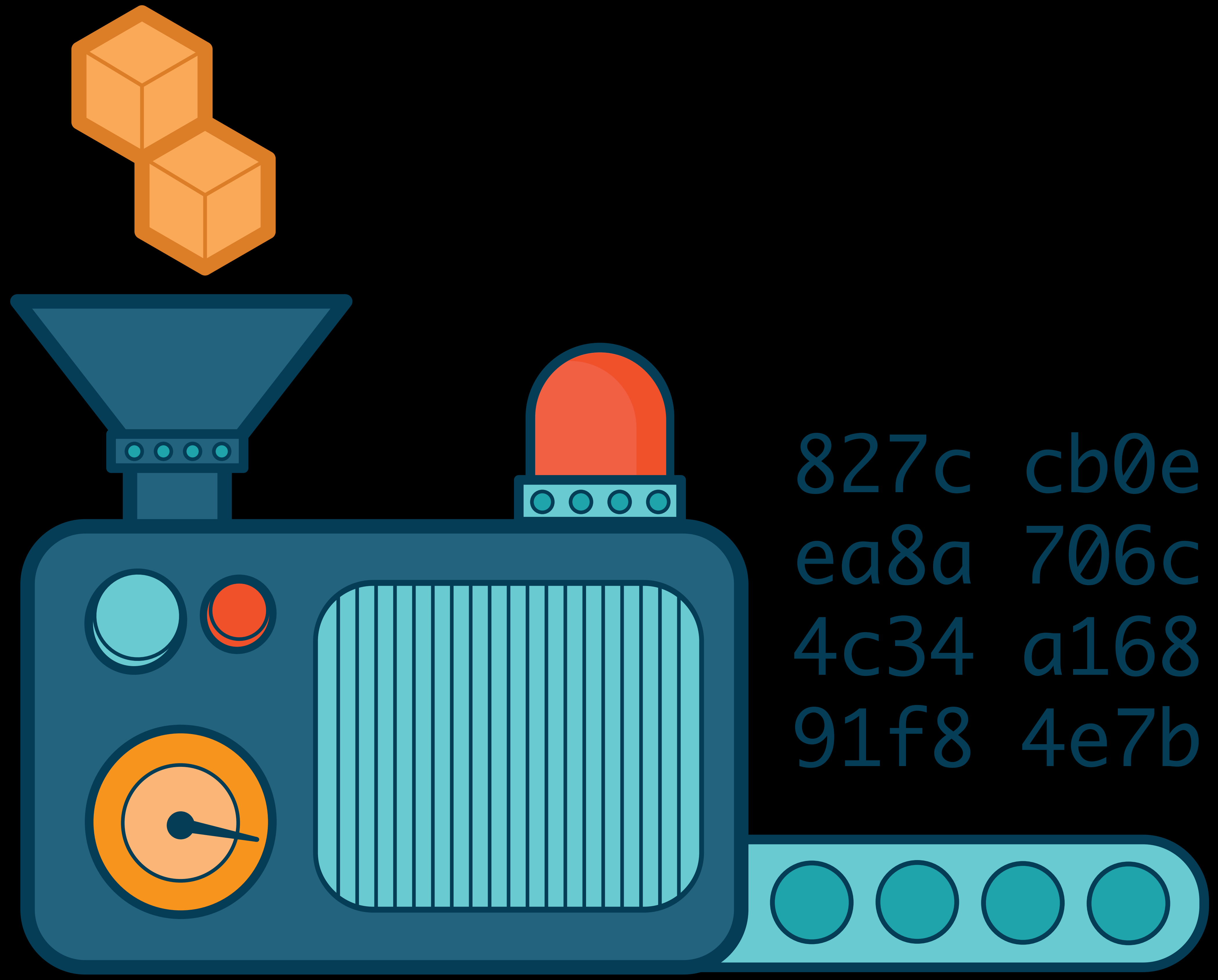
IPFS

5,000,000,000+ files

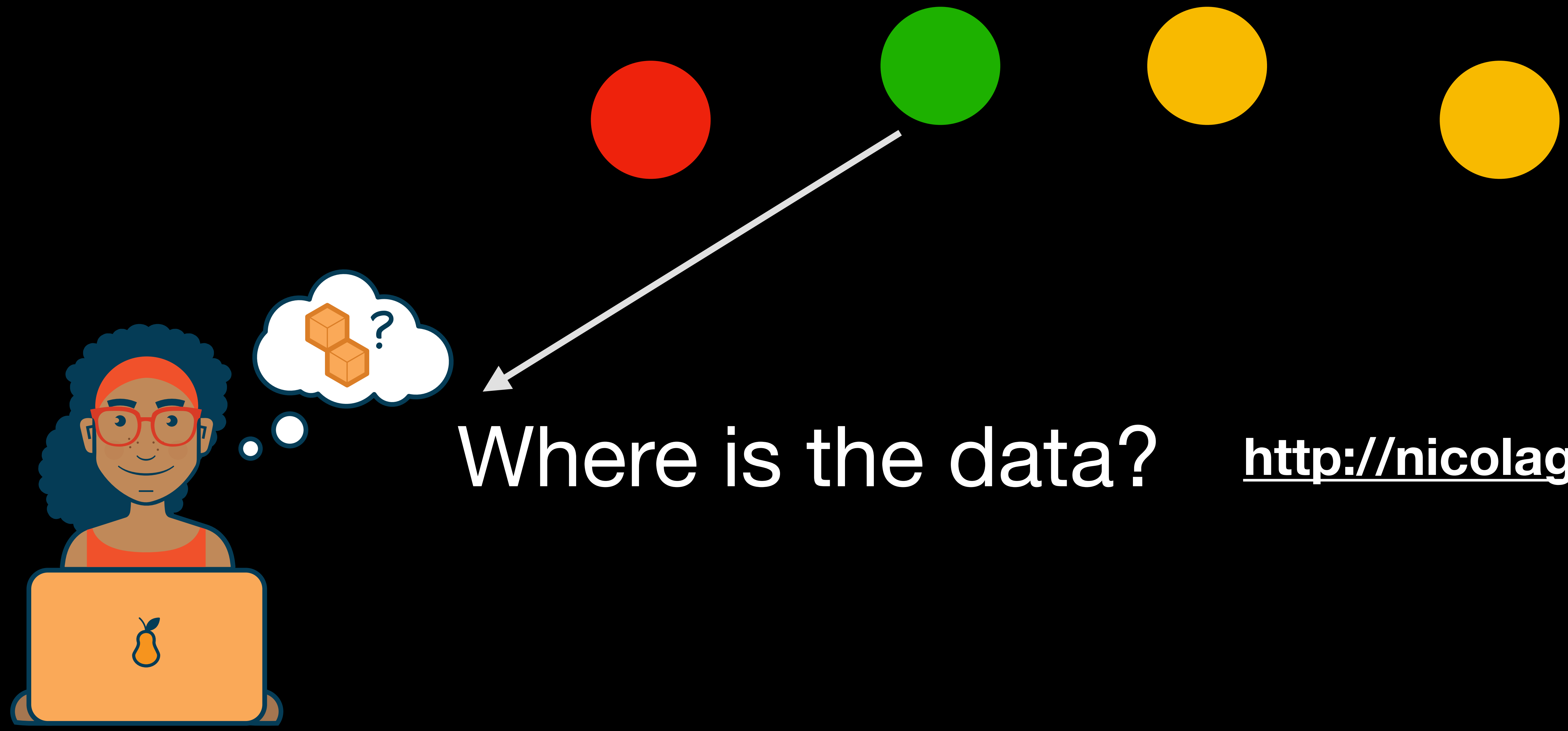
- Video distribution & streaming
- Legal documents
- 3D Models (they’re big!)
- Games
- Scientific data & papers

- Blogs & websites
- Within blockchains
- Totally distributed web apps
  ex. forums, chat, messaging, cms, blogs, github, …

Content Addressing



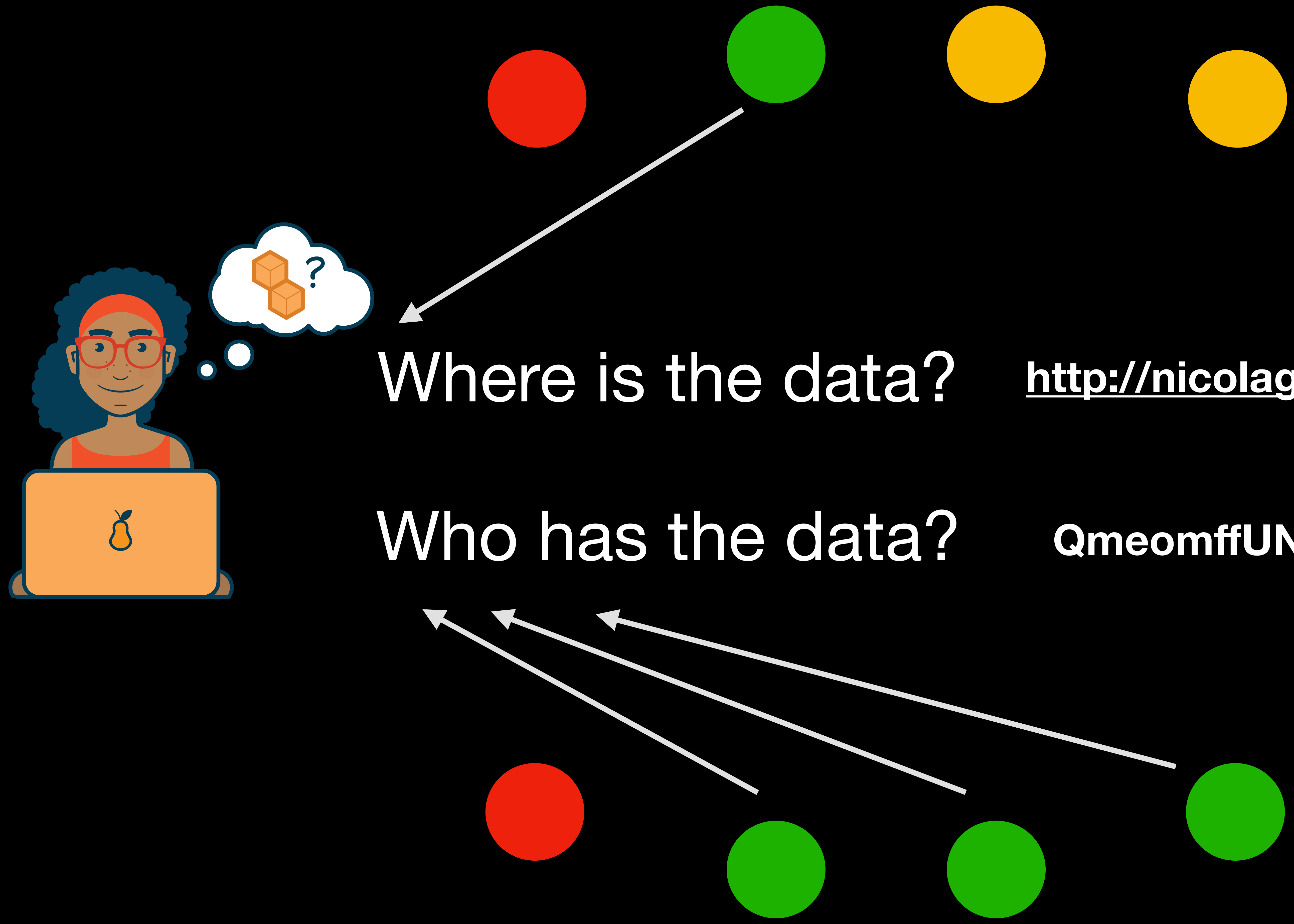
Content Addressing



Where is the data?

http://nicolagreco.com/slides.pdf

Content Addressing



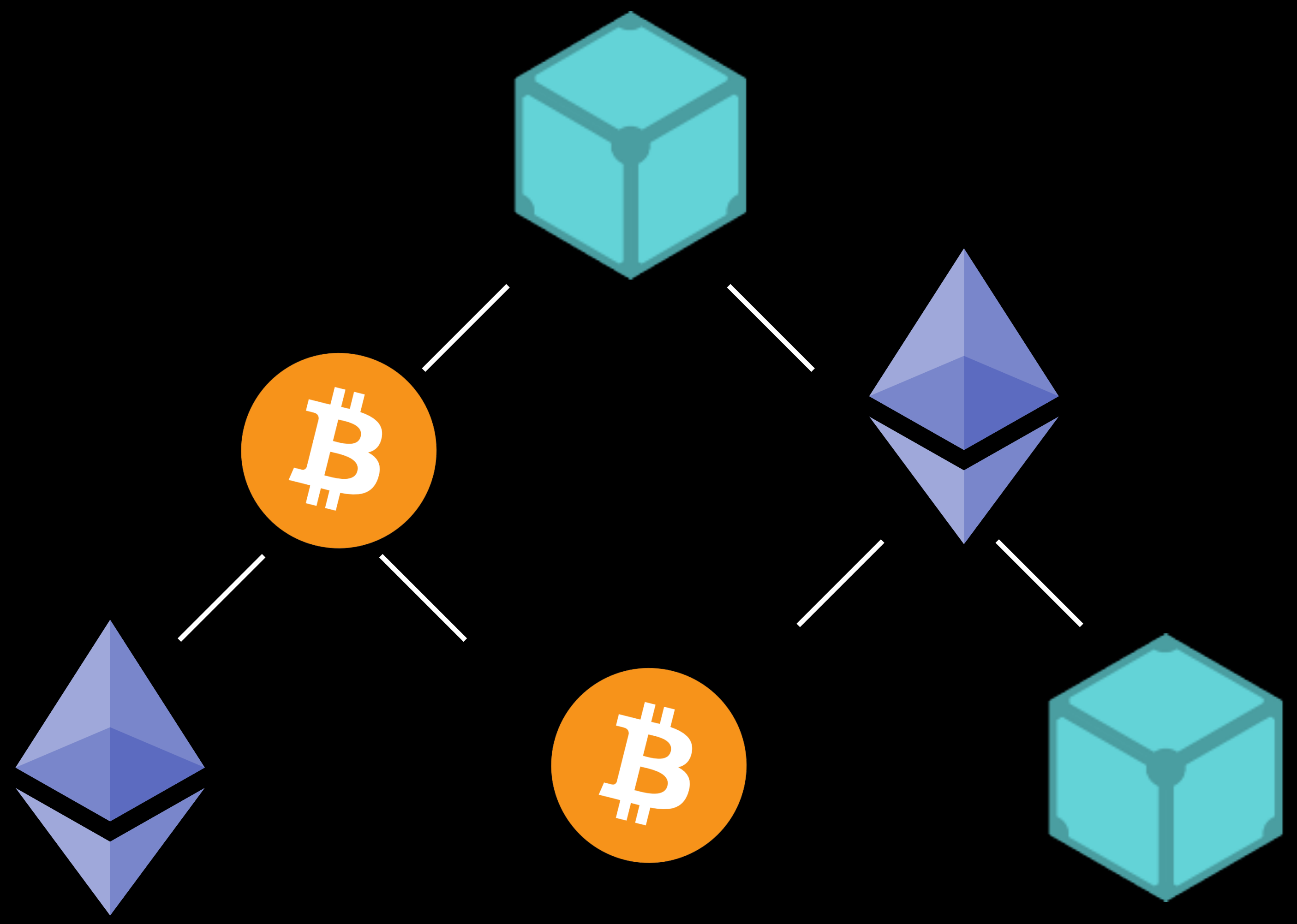
Where is the data? http://nicolagreco.com/slides.pdf

Who has the data? QmeomffUNfmQy76CQGy9N...

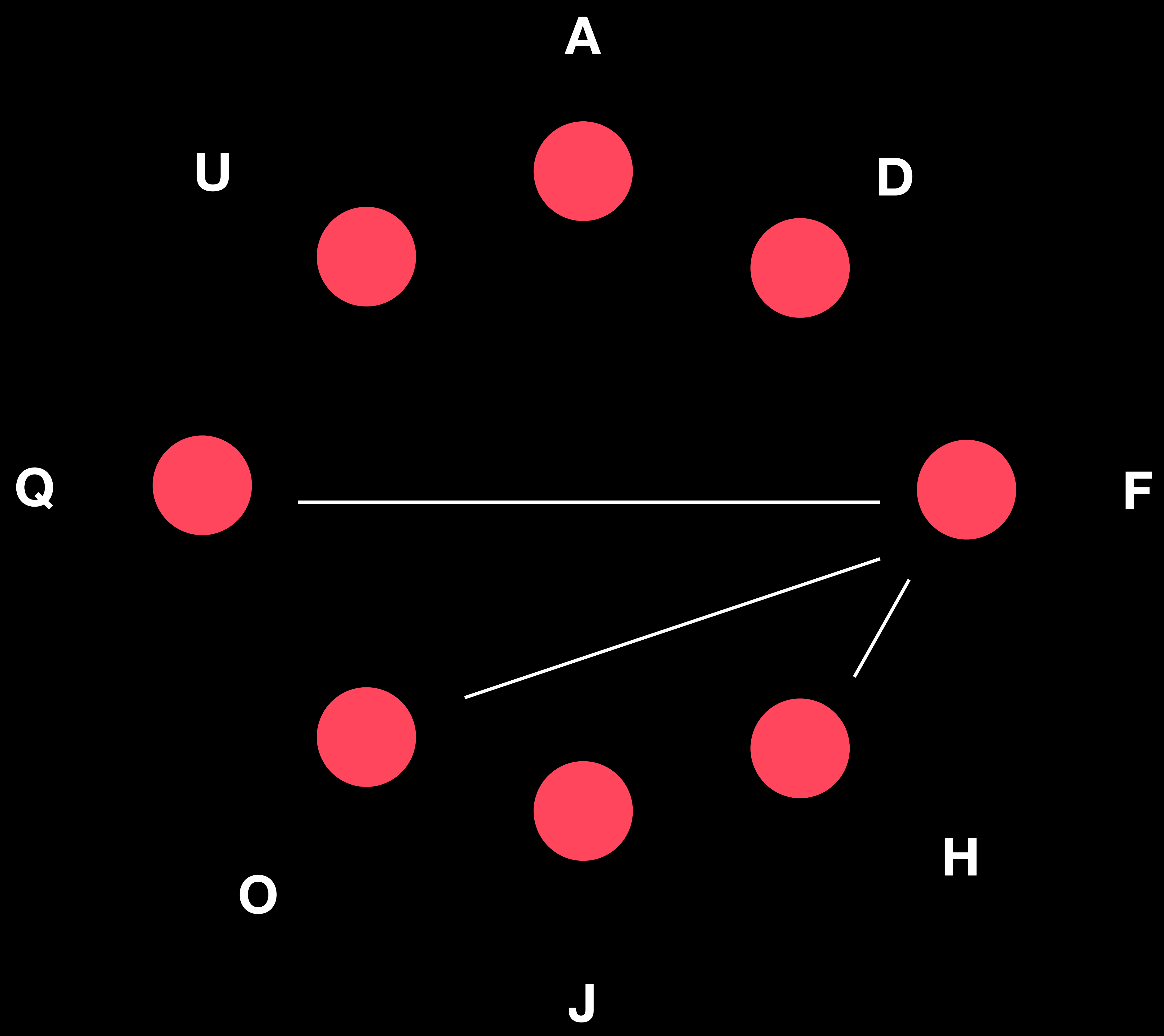
[RFC6920]
[BITTORRENT]
[IPFS]
[BITCOIN]

Content-addressable Web where:

- data links work across application
- links are cryptographic hashes
- anyone can distribute data



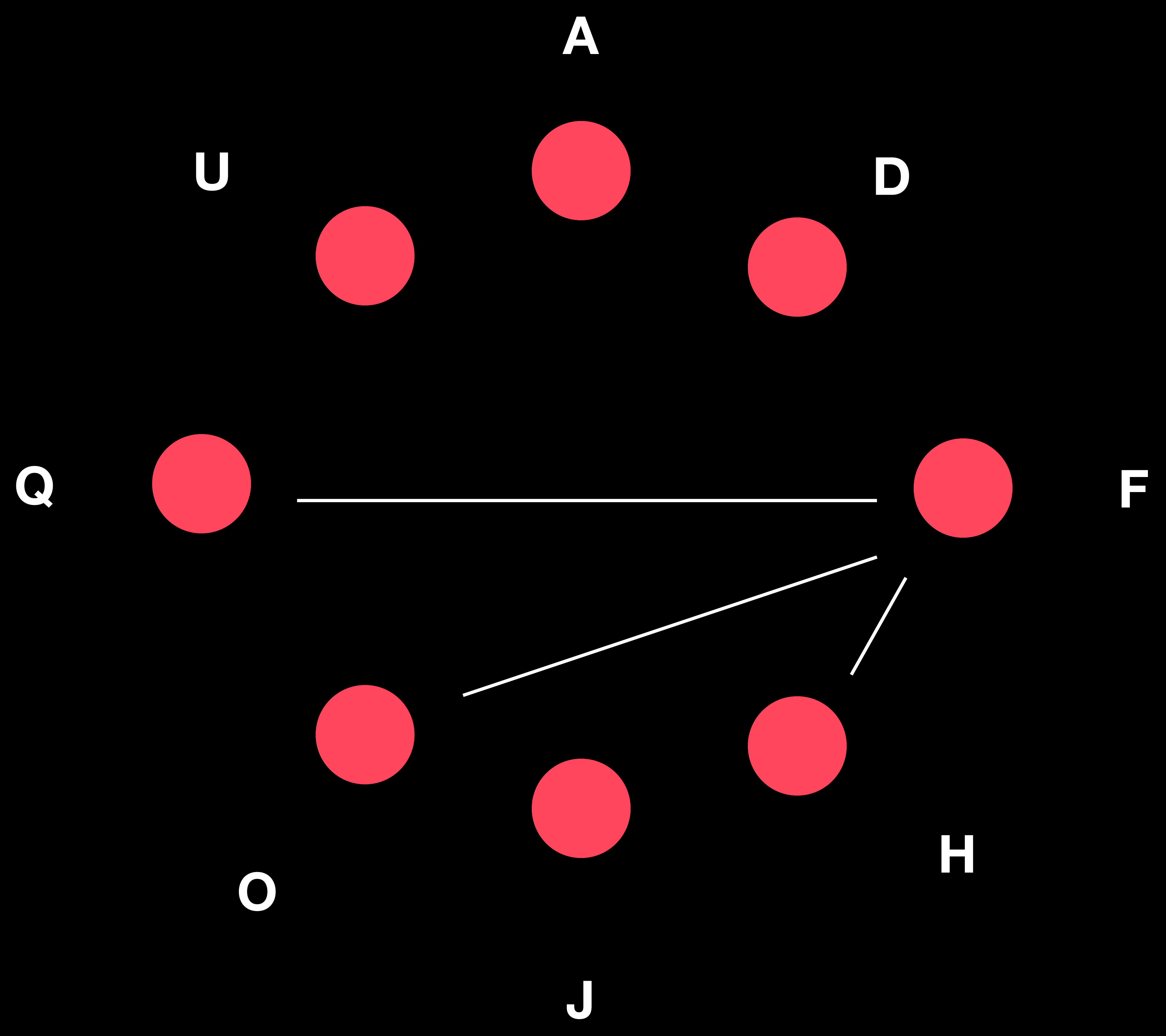
DHT



[CHORD]

DHT

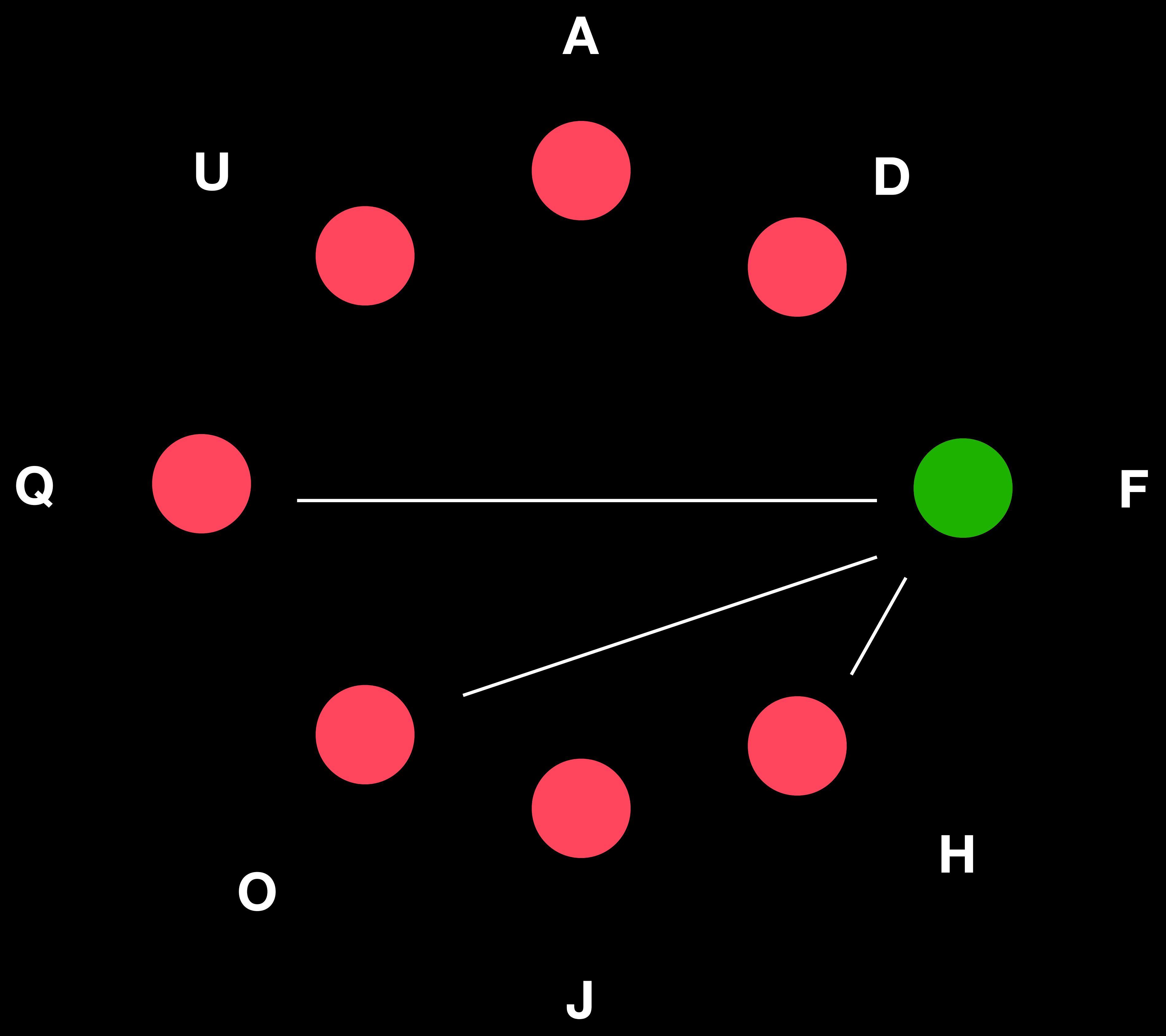
SHA256( ) = GRxQ123..



[CHORD]

DHT

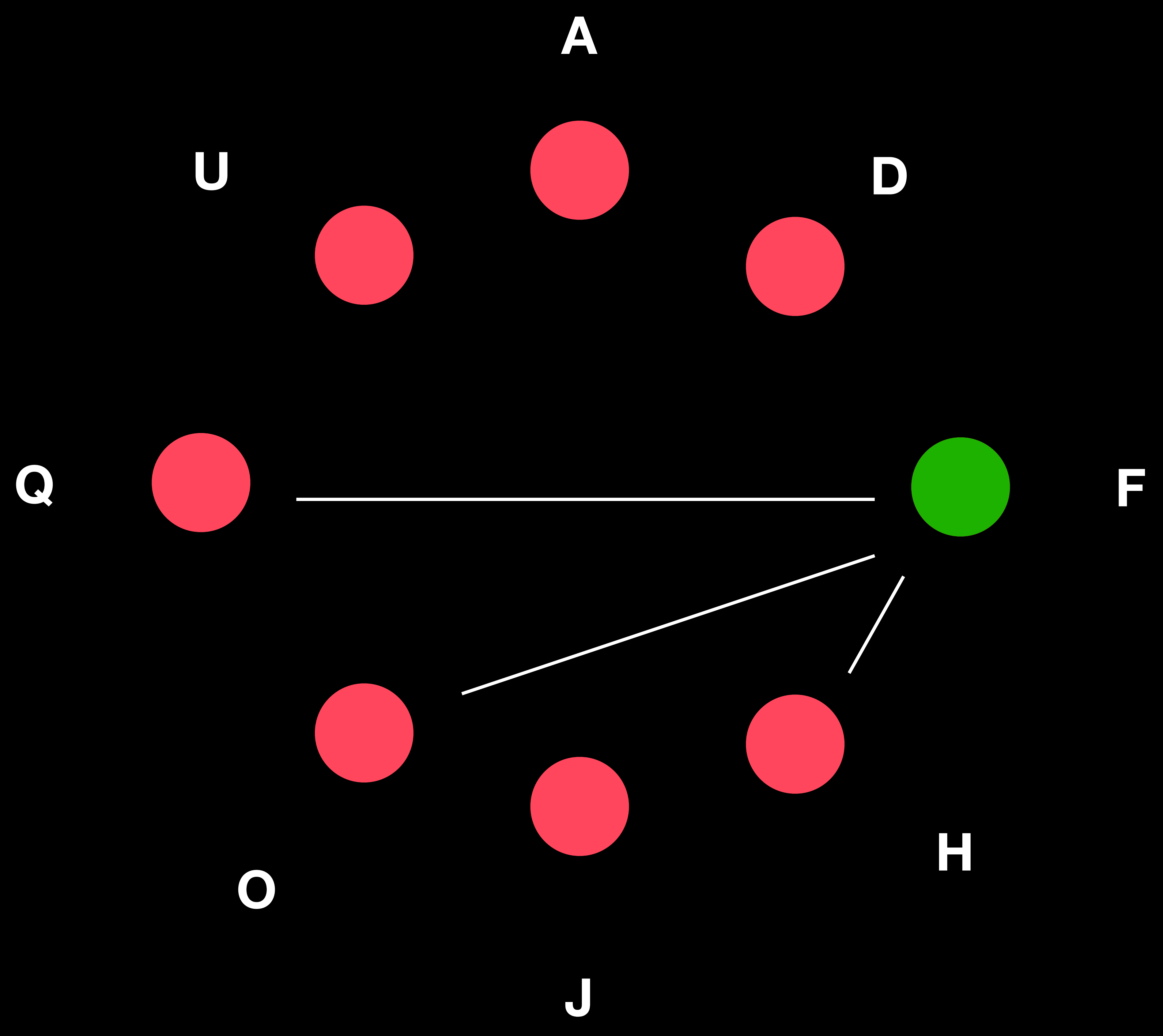
SHA256( ) = GRxQ123..



[CHORD]

DHT

SHA256( ) = GRxQ123..



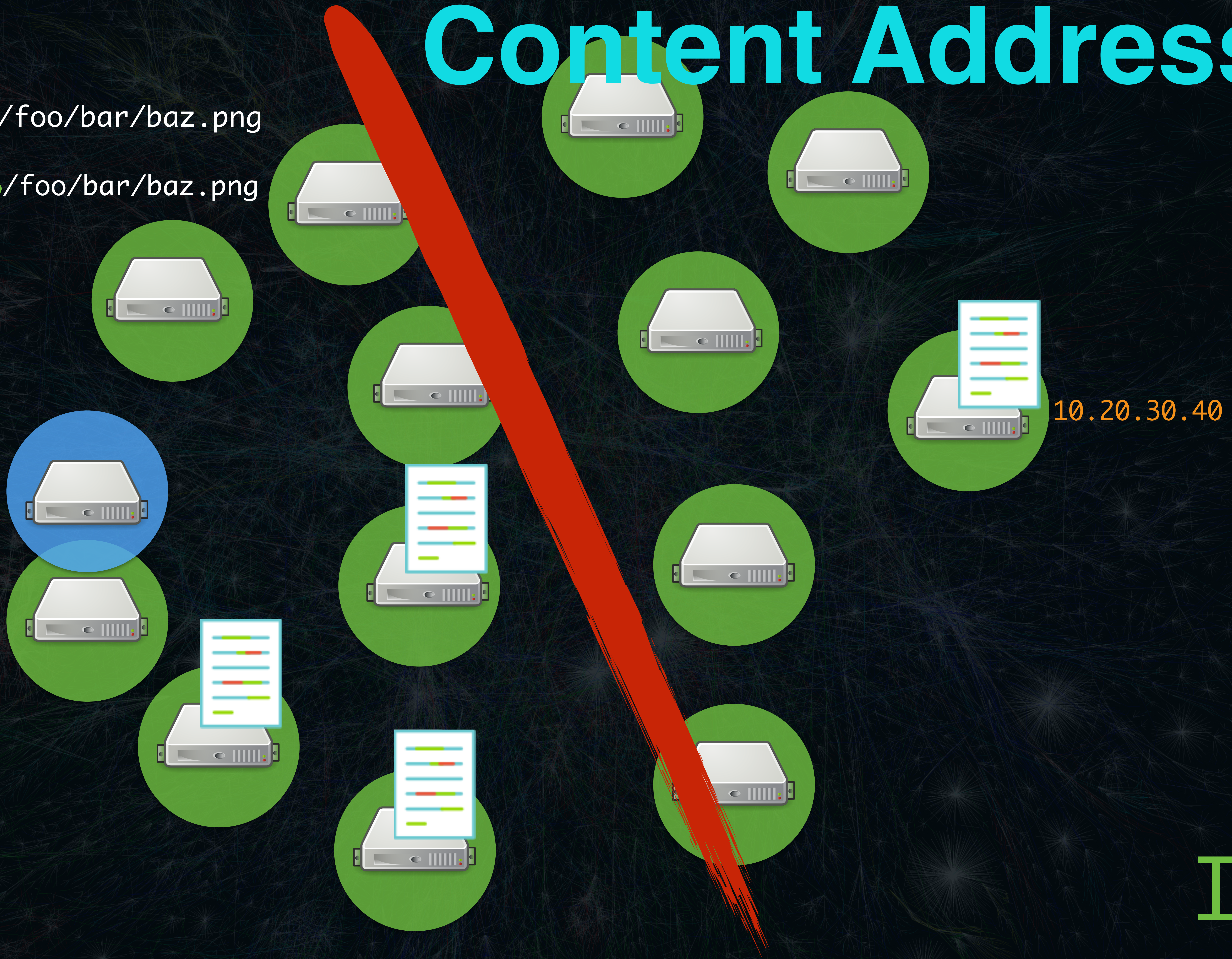
LIBP2P

[CHORD]

Content Addressing

http://10.20.30.40/foo/bar/baz.png

/ipfs/QmW98pJrc6FZ6/foo/bar/baz.png



IPFS

IPFS

IPFS .JS

Large Open Source Project
Over 2000+ Contributors
Over 150+ contribute Weekly

live ipfs network already distributed all over the world

Norwegian Sea
IS
SE
FI
NO
Russia
Canada
DK
IE
UK
BY
PL
DE
UA
FR
HU
RO
Kazakhstan
Mongolia
North
Atlantic
Ocean
United
States
ES
IT
GR
Turkey
UZ
KG
TM
TJ
Japan
China
MA
TN
SY
IQ
Iran
AF
KW
Algeria
Libya
Egypt
Saudi
Arabia
PK
NP
Mexico
CU
BD
India
OM
MM
LA
MR
Mali
Niger
Arabian
Sea
SN
TD
Sudan
RY
TH
VN
PH
Venezuela
GH
NG
SS
ET
SO
LK
Colombia
CM
KE
MV
Malaysia
EC
CD
Indonesia
TZ
PG
Peru
Brazil
AO
Bolivia
MZ
MG
Indian
Ocean
Coral Sea
BW
PY
South
Atlantic
Ocean
Australia
South
Pacific
Ocean
South
Africa
UY
Argentina
CL
Tasman
Sea
NZ

Web

Server <> Client

Server provides the right service
Server uses data responsibly
Server is secure
Server is always online
Server is single point of reference

P2P

Server <> Server

Altruistic Network
Peers are equal

Incentivized Protocols

Network <> Client

Clients delegate their service to the network
The network is “paid” to do so

IPFS

(altruistic)

IPFS

(altruistic)

Filecoin

(incentivized)

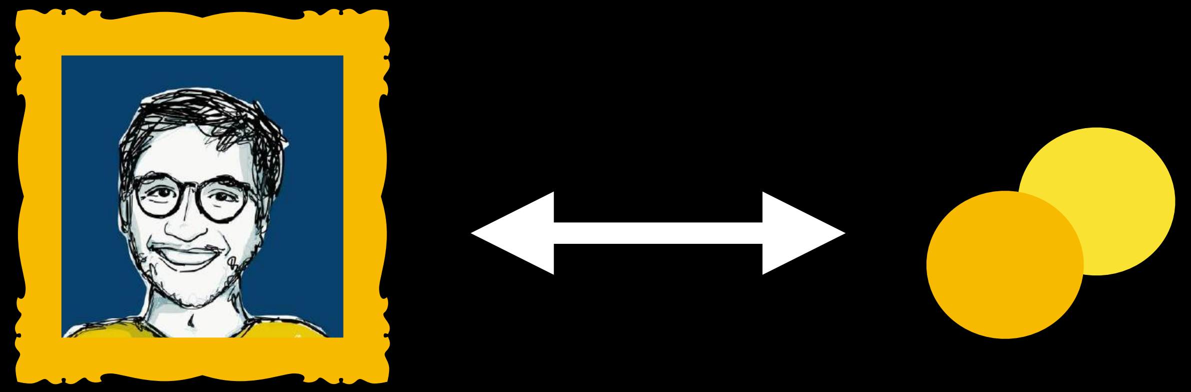
Part 2

Universal Services

decentralization beyond the web

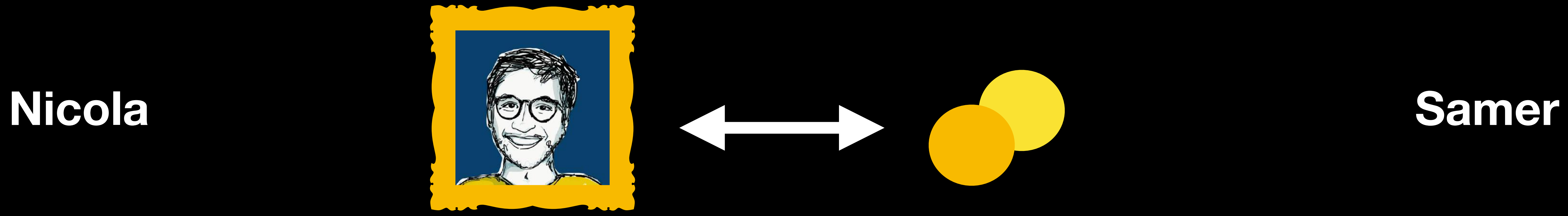
Fair Exchange

Nicola



Samer

Fair Exchange

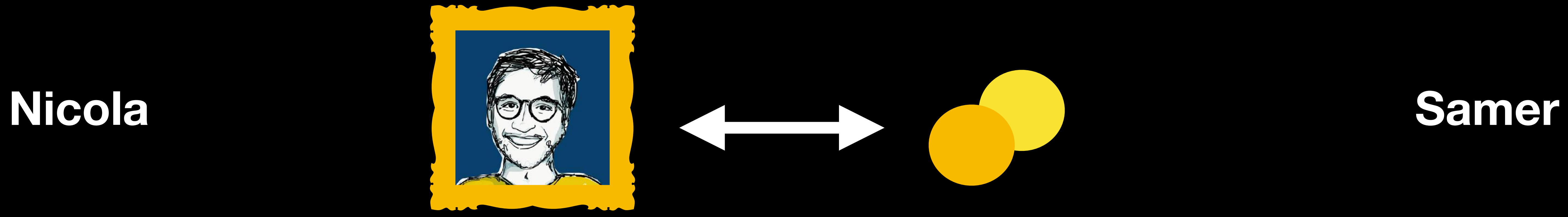


Nicola

Samer

Fairness Either both parties receive their inputs or none

Fair Exchange



Nicola

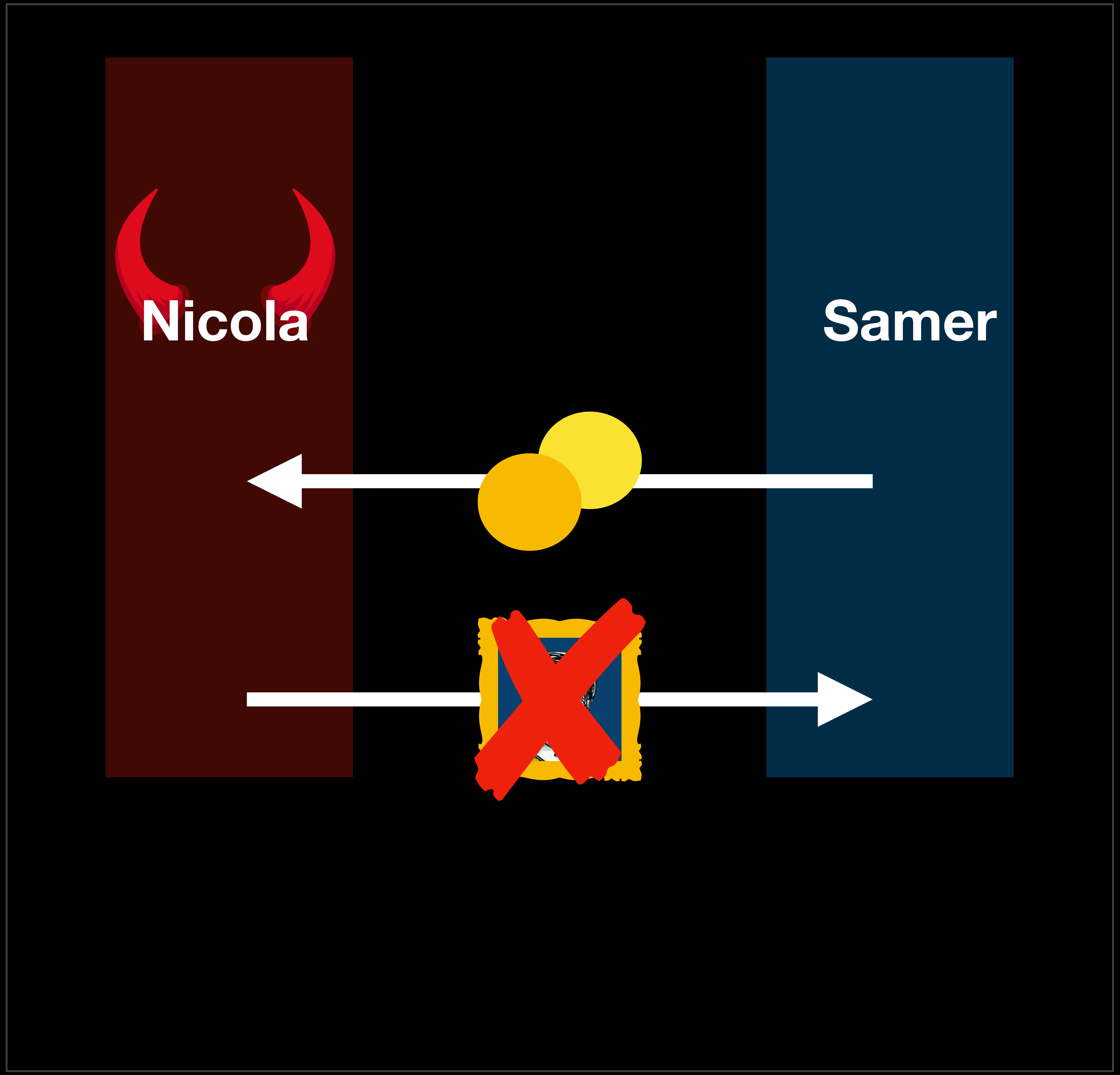
Samer

Fairness Either both parties receive their inputs or none

Timeliness Exchange either happens or does terminate

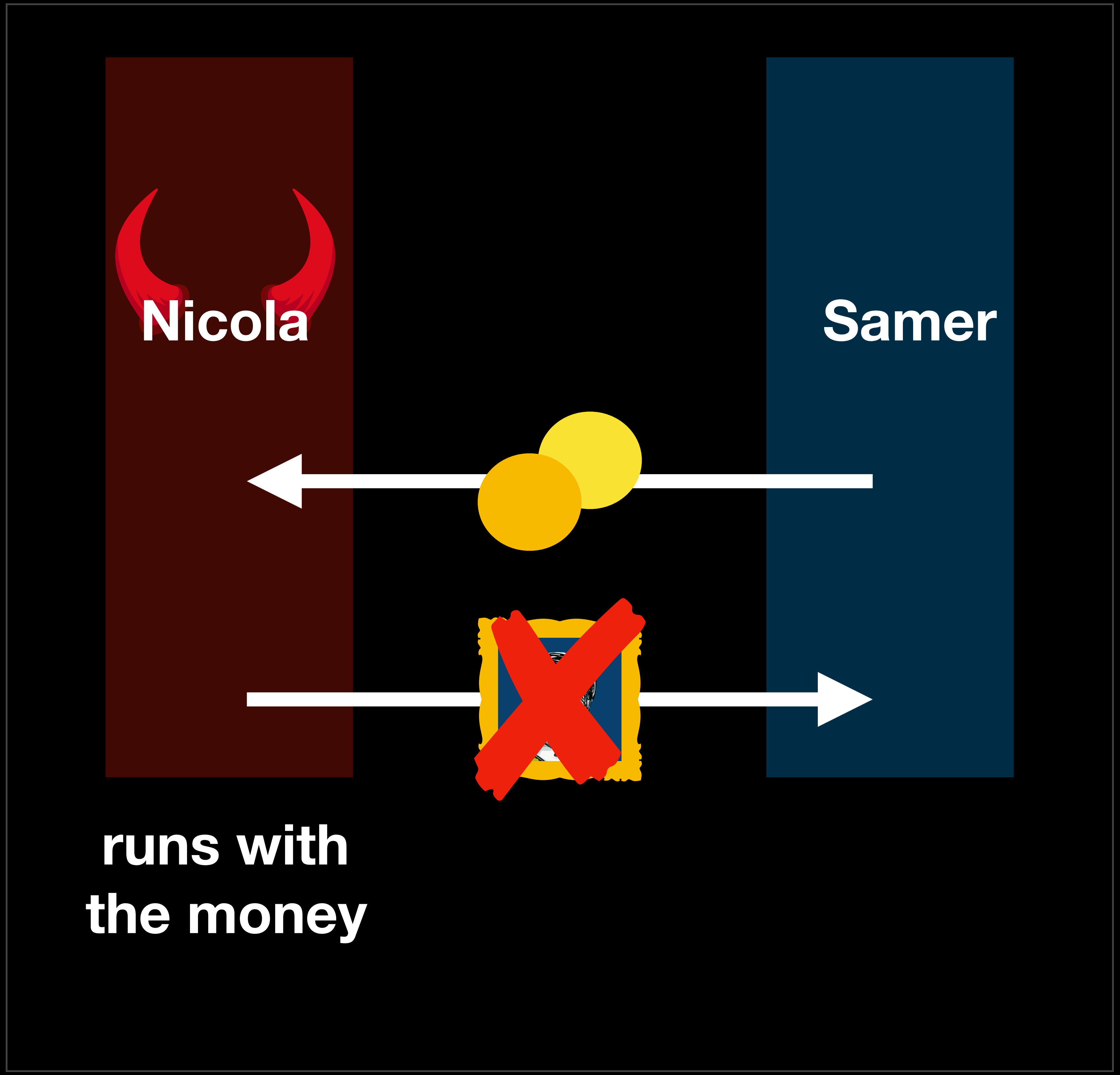
Fair Exchange

Scenario 1



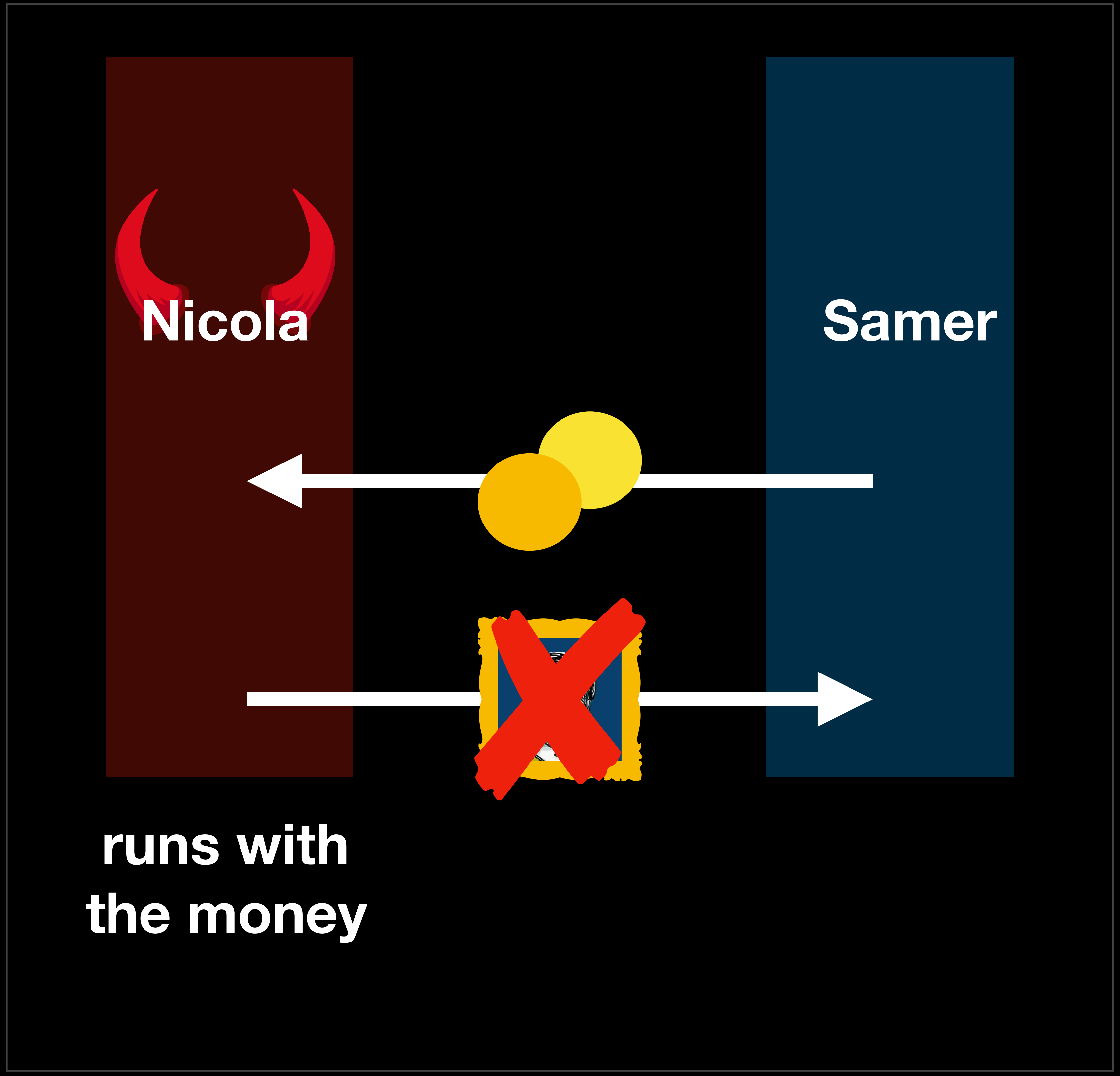
Fair Exchange

Scenario 1

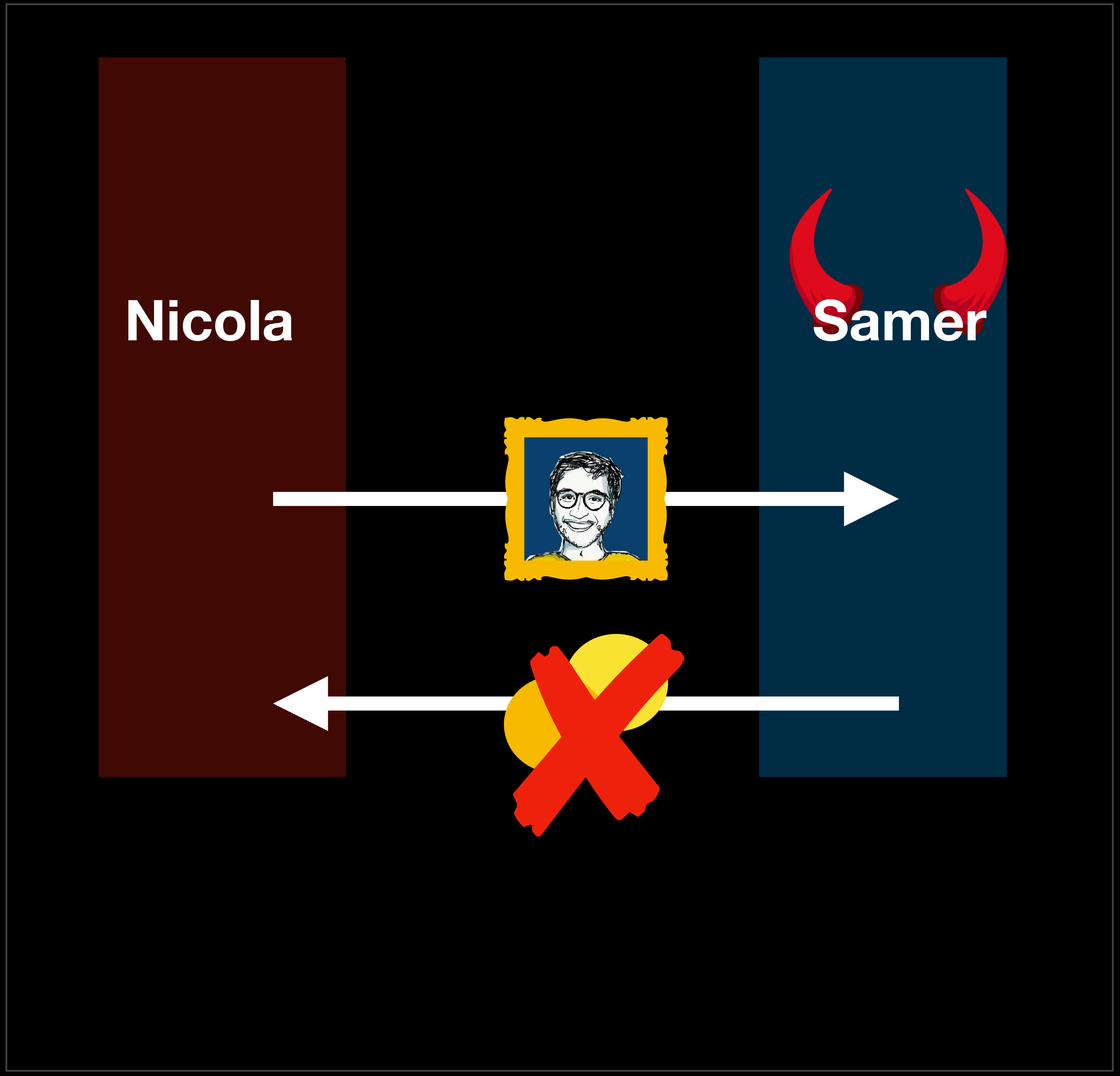


Fair Exchange

Scenario 1

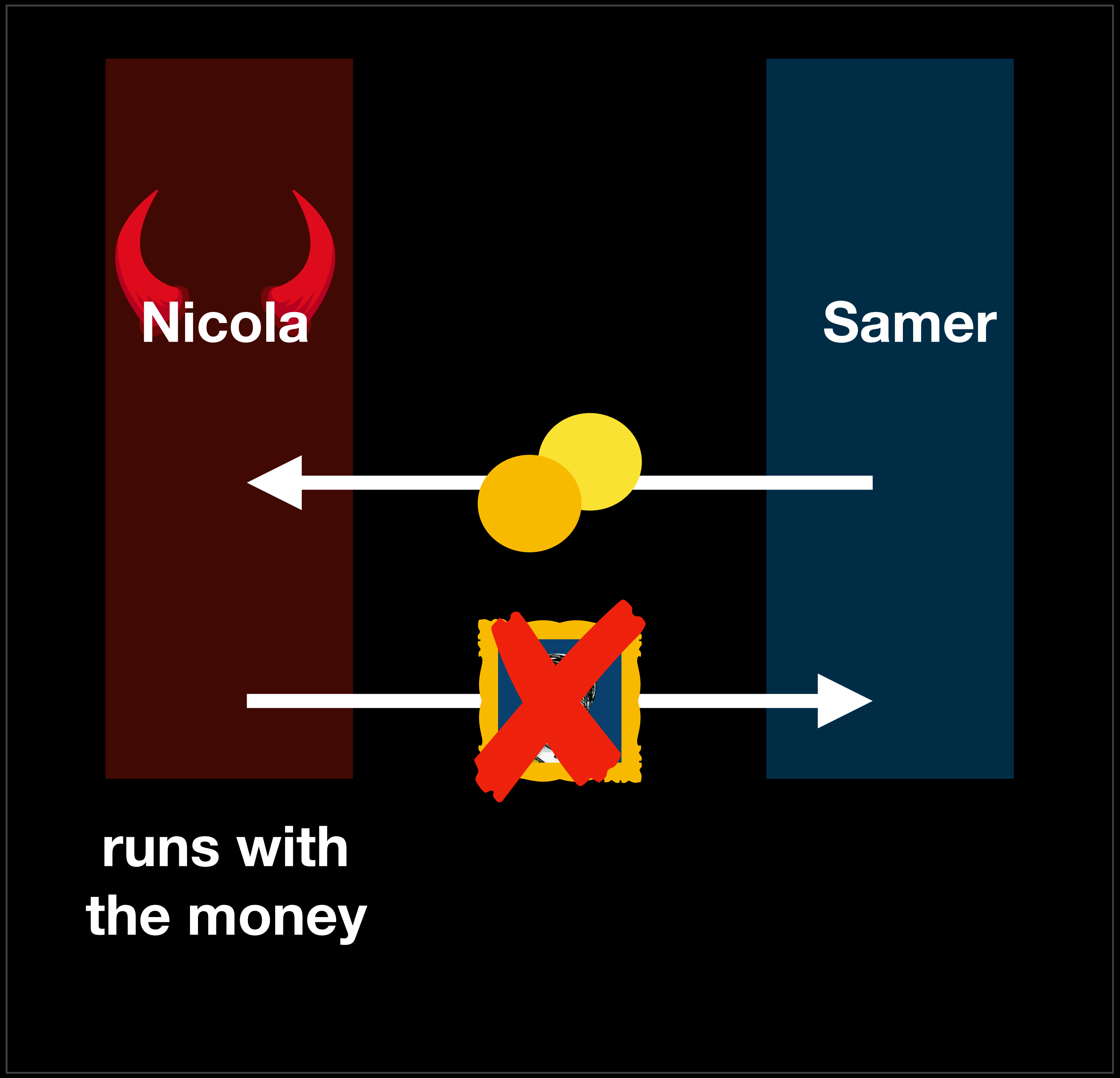


Scenario 2

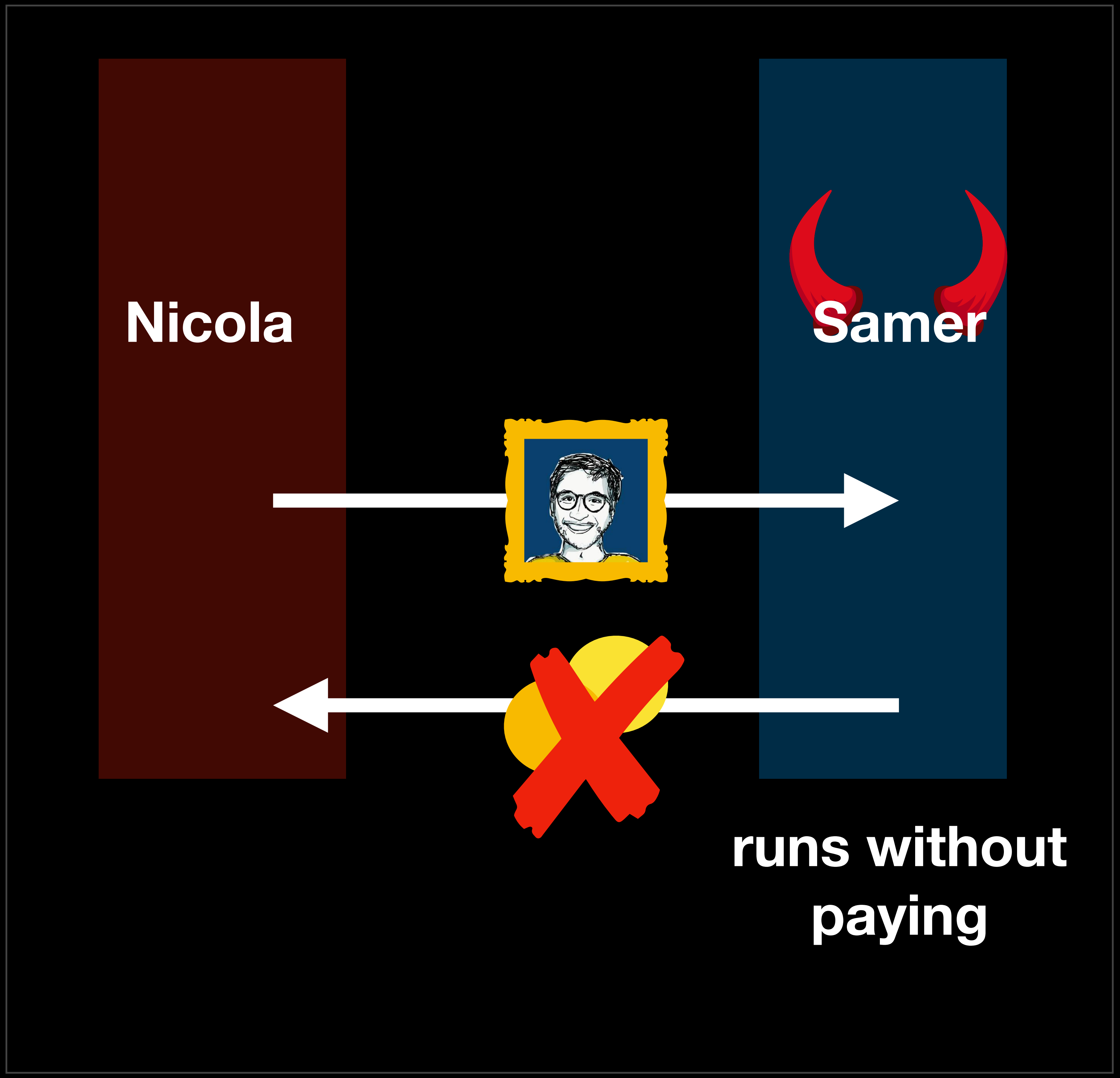


Fair Exchange

Scenario 1

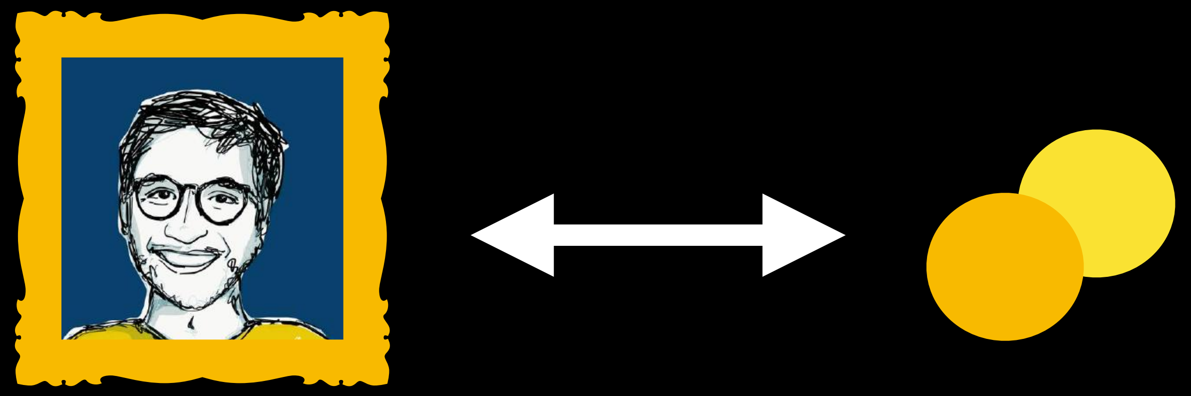


Scenario 2



Fair Exchange

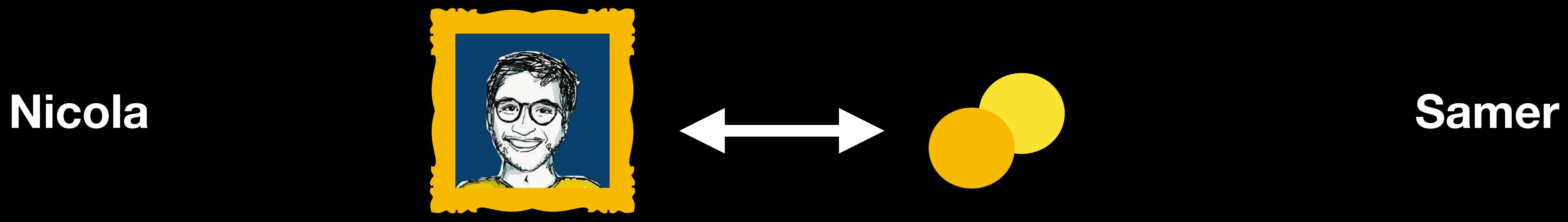
Nicola



Samer

[Cleve1986]

Fair Exchange



Nicola

Samer

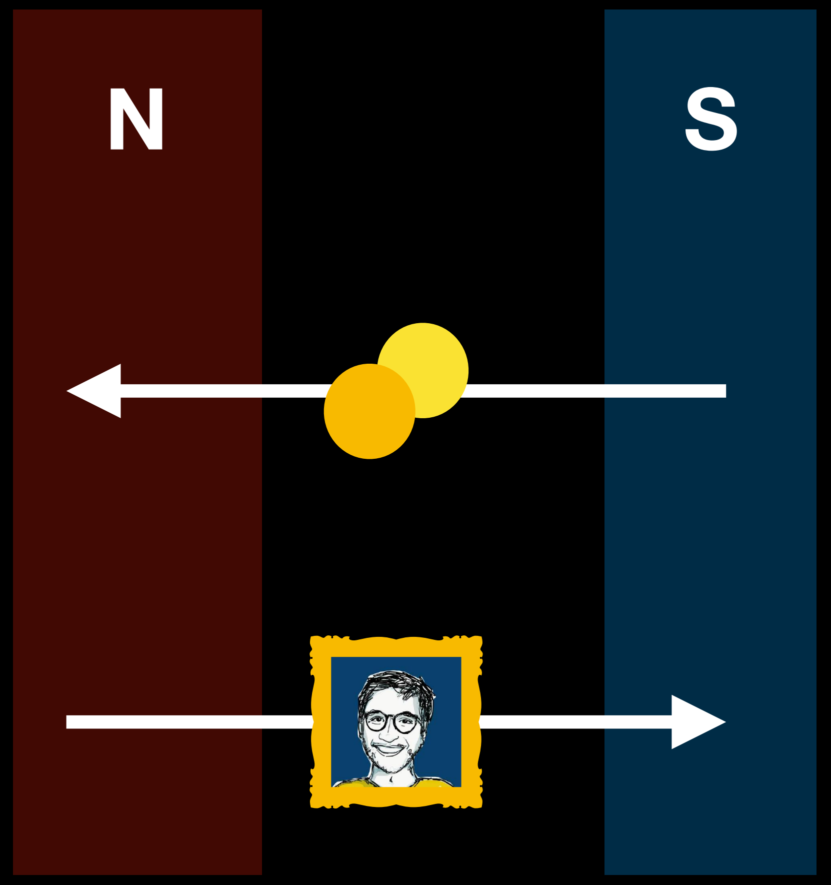
Impossibility of Fair Exchange without a Trusted Third Party

[Cleve1986]

Fair Exchange

— Trust Assumptions —

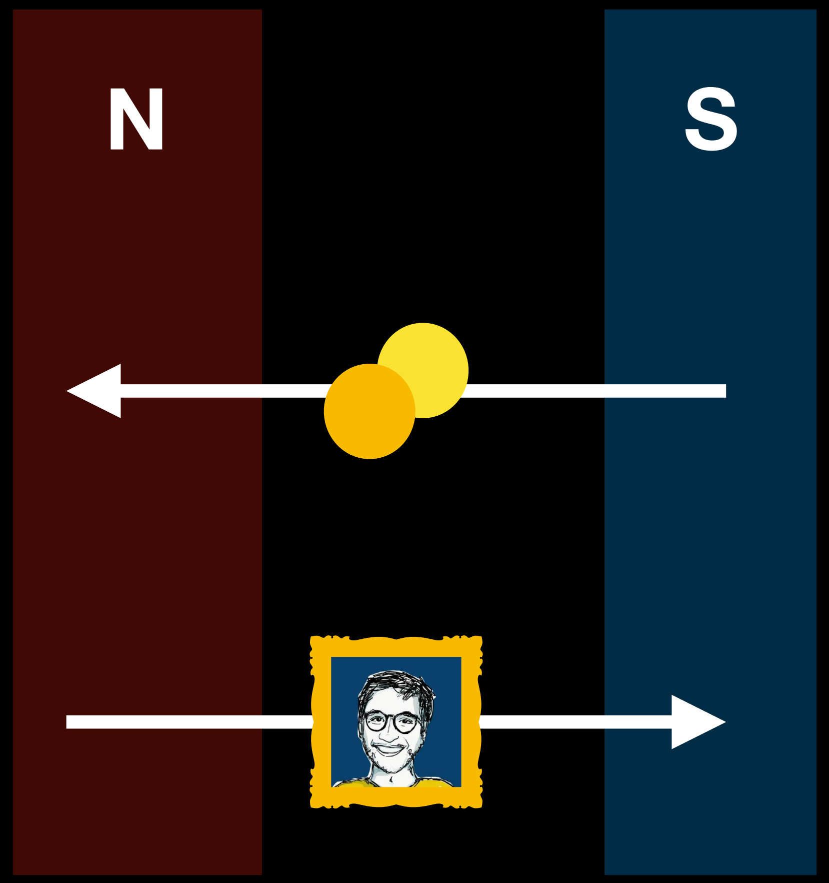
Trusted



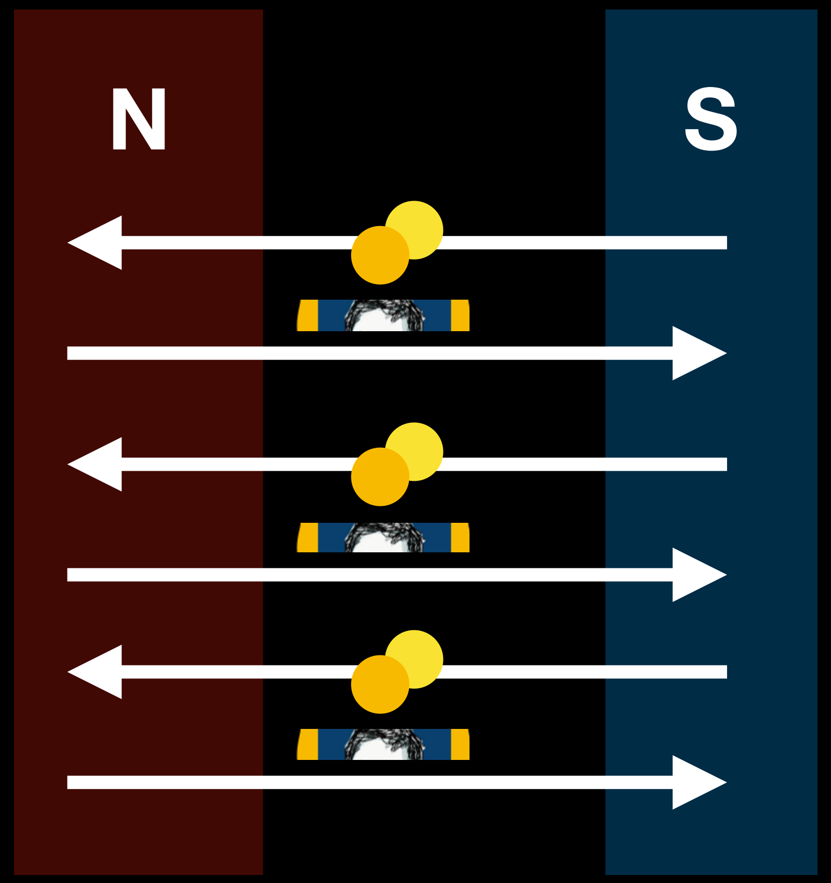
Fair Exchange

— Trust Assumptions —

Trusted

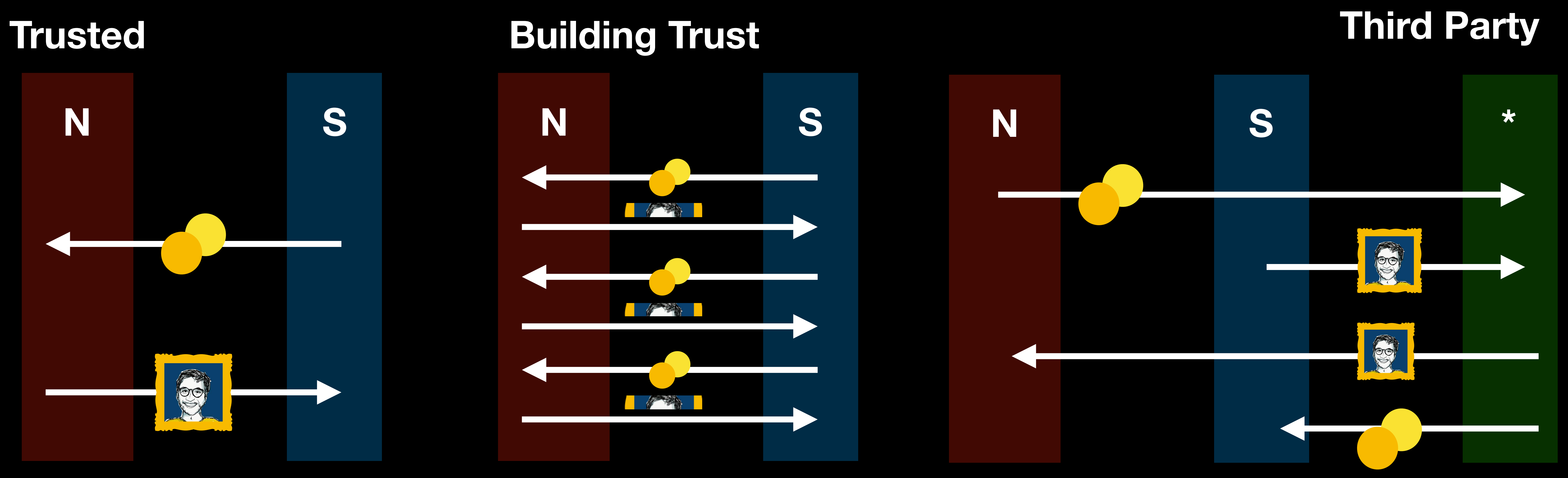


Building Trust



Fair Exchange

— Trust Assumptions —



Fair Exchange

— Trust Assumptions —

Trusted
Party

Fair Exchange

— Trust Assumptions —

Trusted Party

Trusted Hardware

Fair Exchange

— Trust Assumptions —

Trusted Party

Trusted Hardware

Trusted Auditors

Fair Exchange

— Trust Assumptions —

Trusted Party

Trusted Hardware

Trusted m-of-n

Trusted Auditors

Fair Exchange

— Trust Assumptions —

Trusted Party

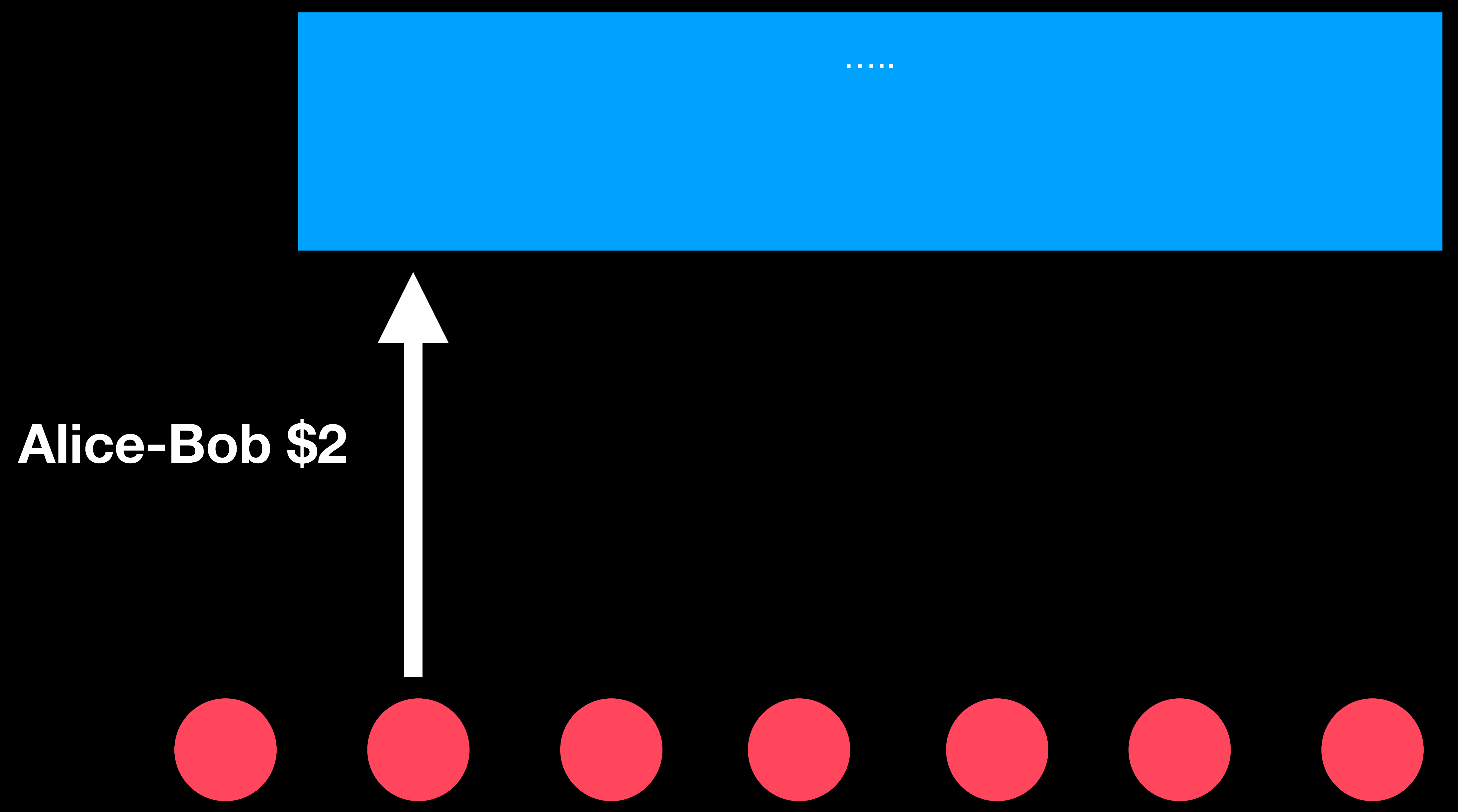
Trusted Hardware

Trusted Majority

Trusted m-of-n

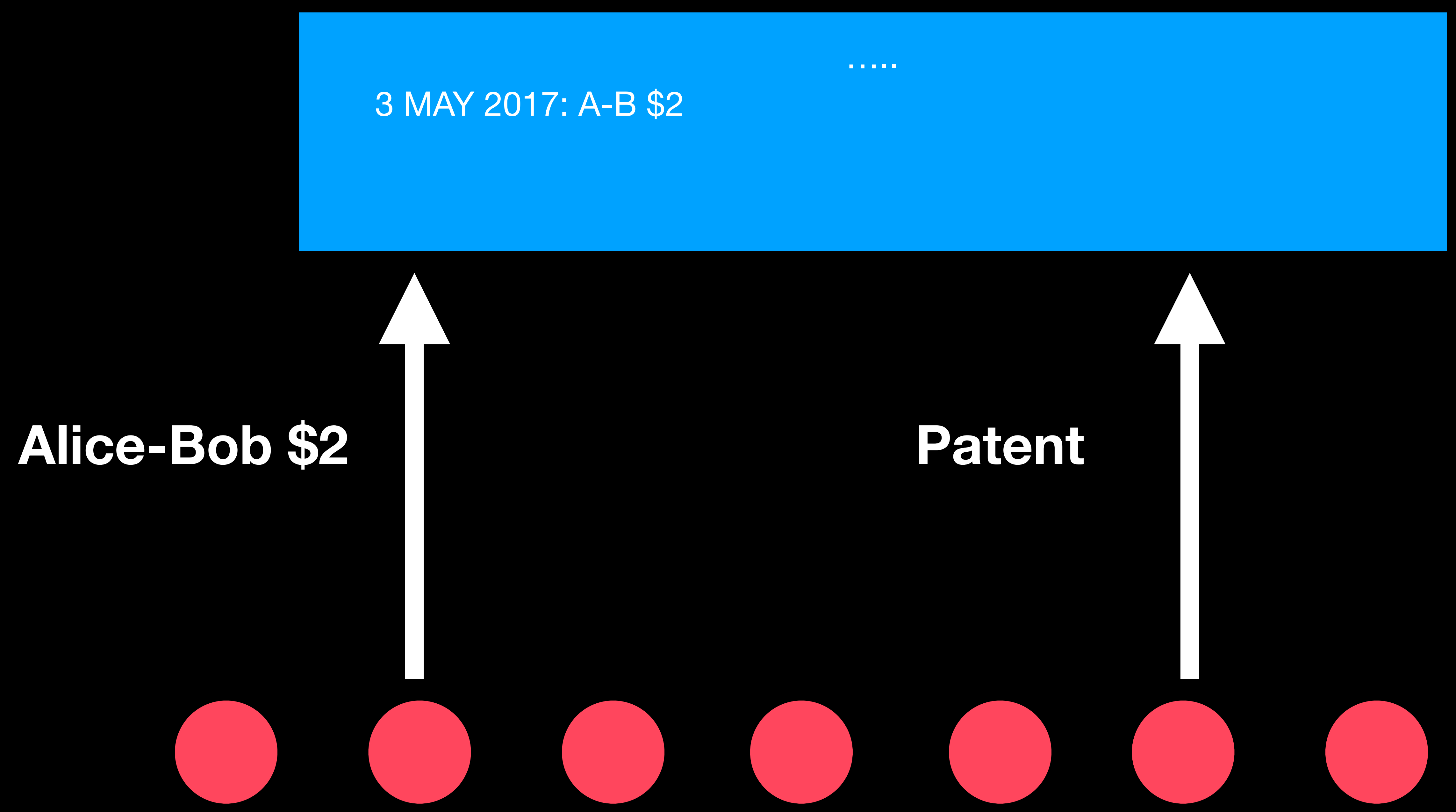
Trusted Auditors

Public Ledger



Alice-Bob $2

Public Ledger



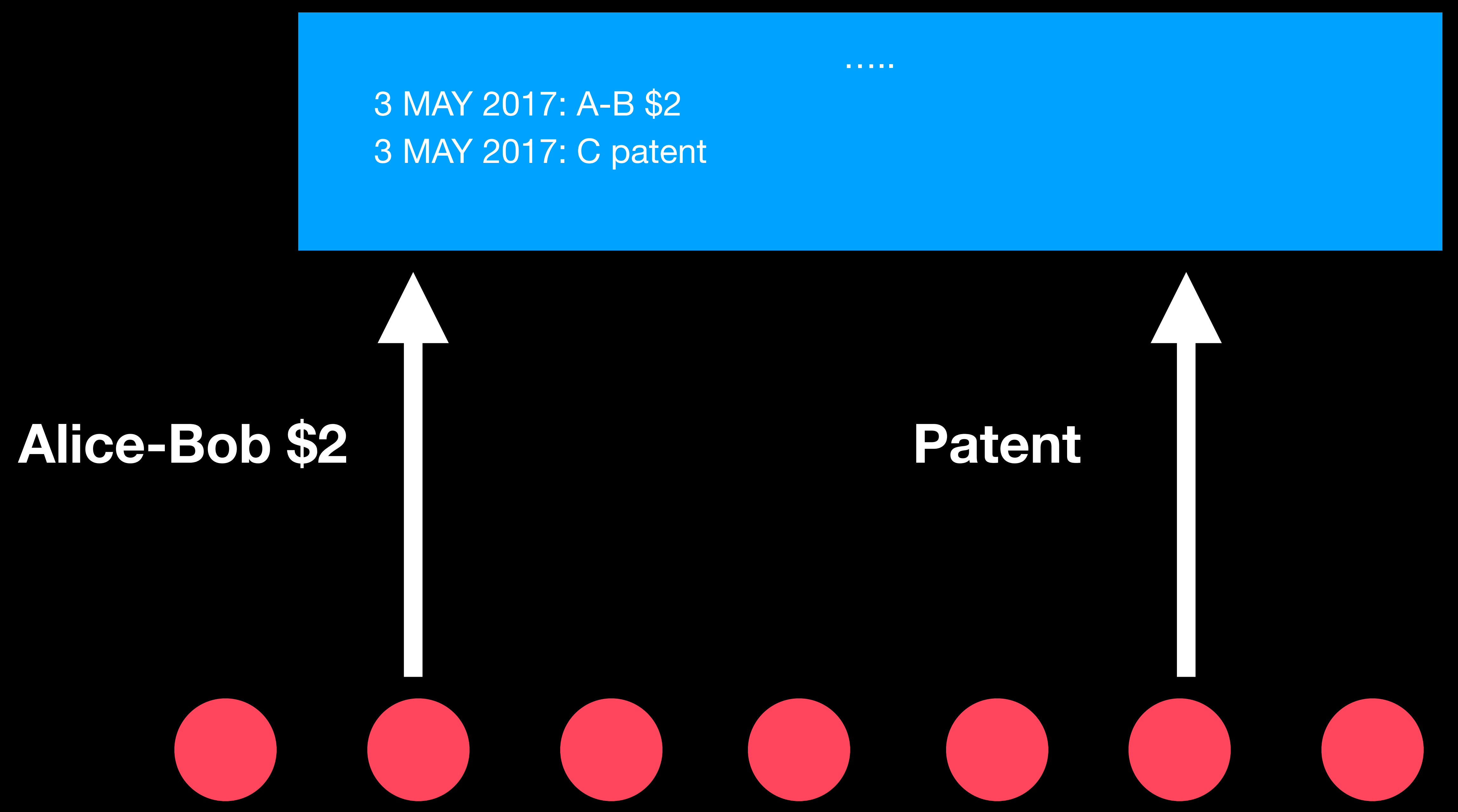
.....

3 MAY 2017: A-B $2

Alice-Bob $2

Patent

Public Ledger



.....

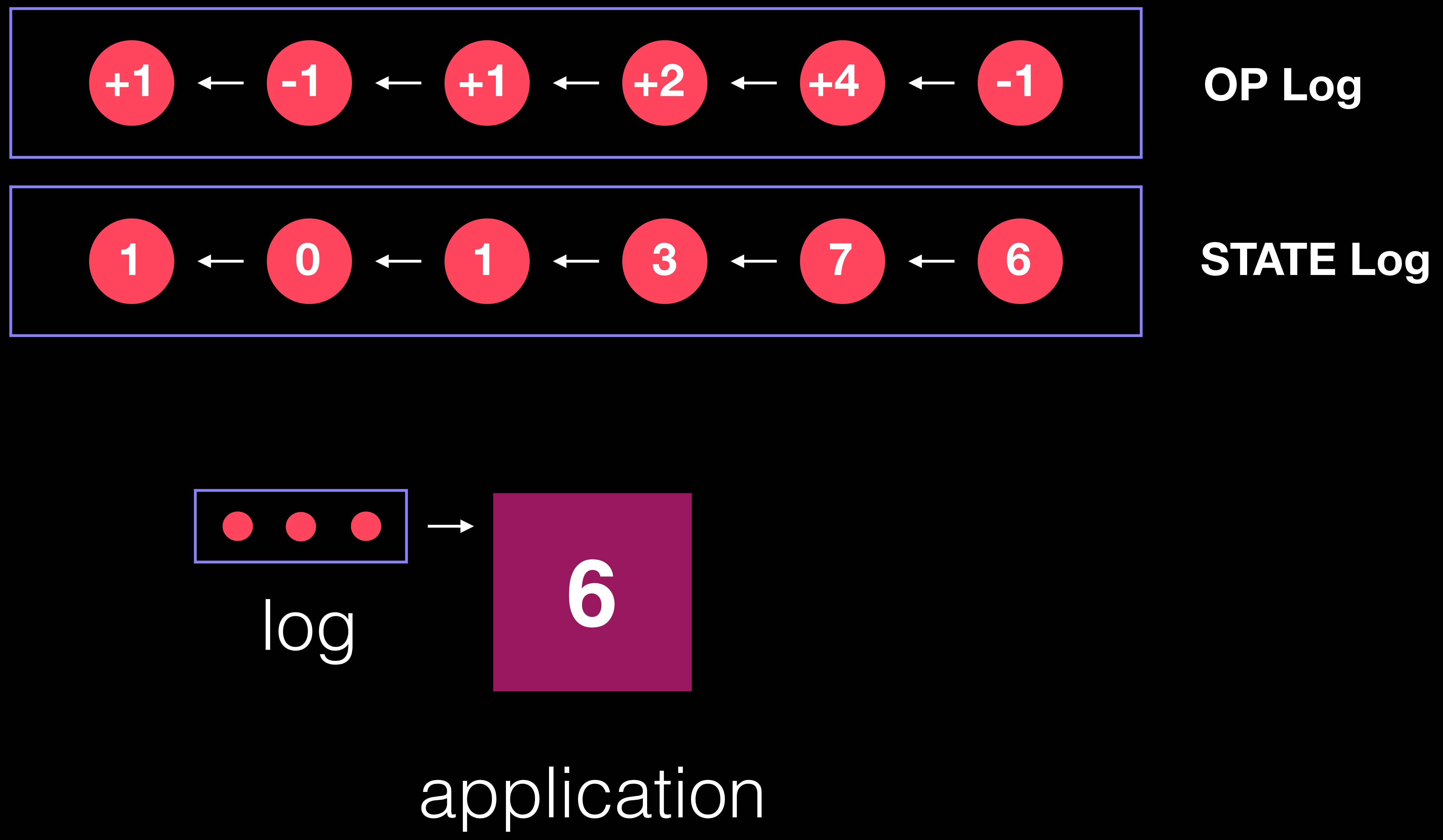
3 MAY 2017: A-B $2

3 MAY 2017: C patent

Alice-Bob $2

Patent

State Machine Replication



+1 ← -1 ← +1 ← +2 ← +4 ← -1 OP Log

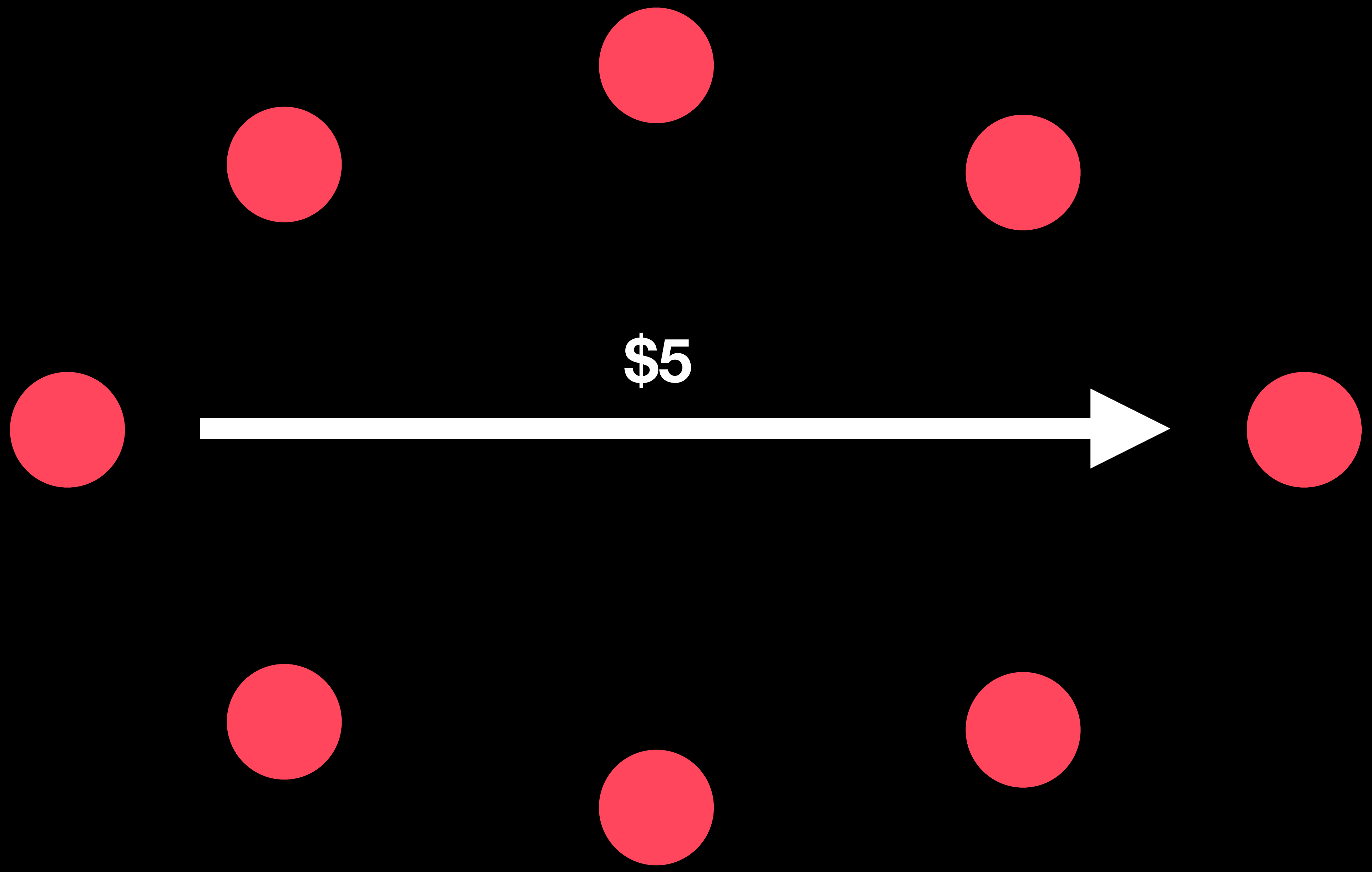
1 ← 0 ← 1 ← 3 ← 7 ← 6 STATE Log

● ● ● → 6

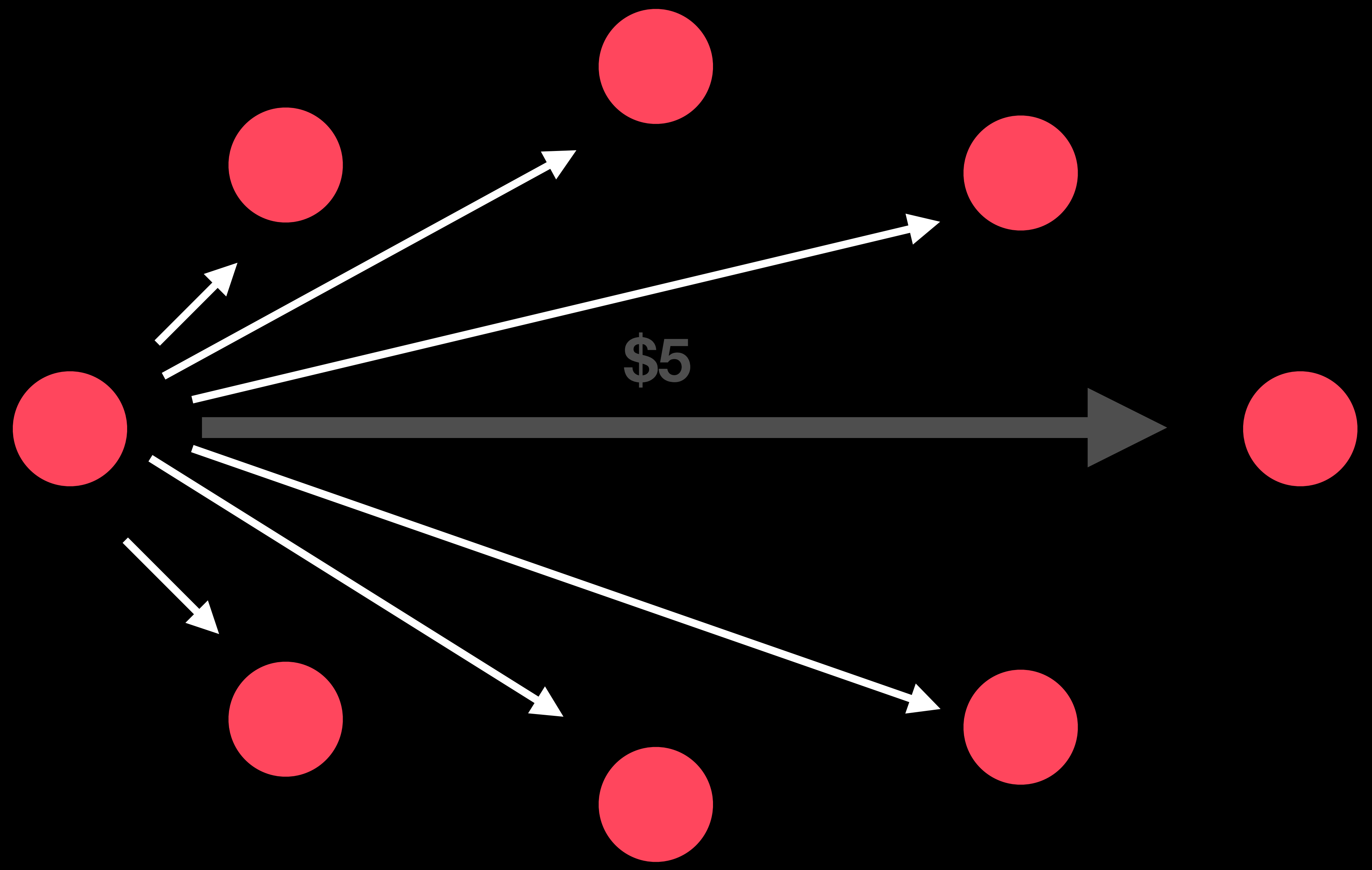
log

application

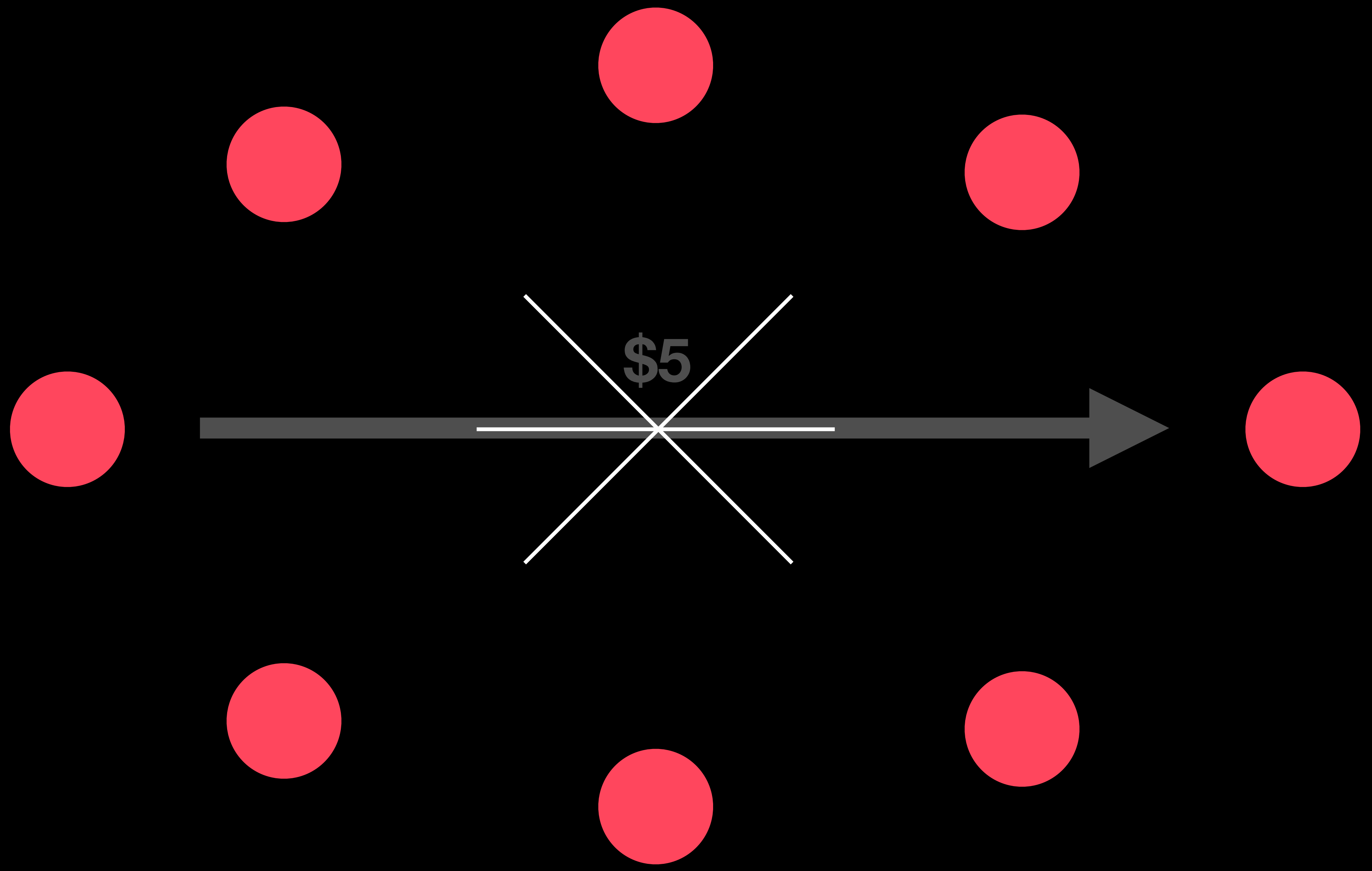
Digital Currency



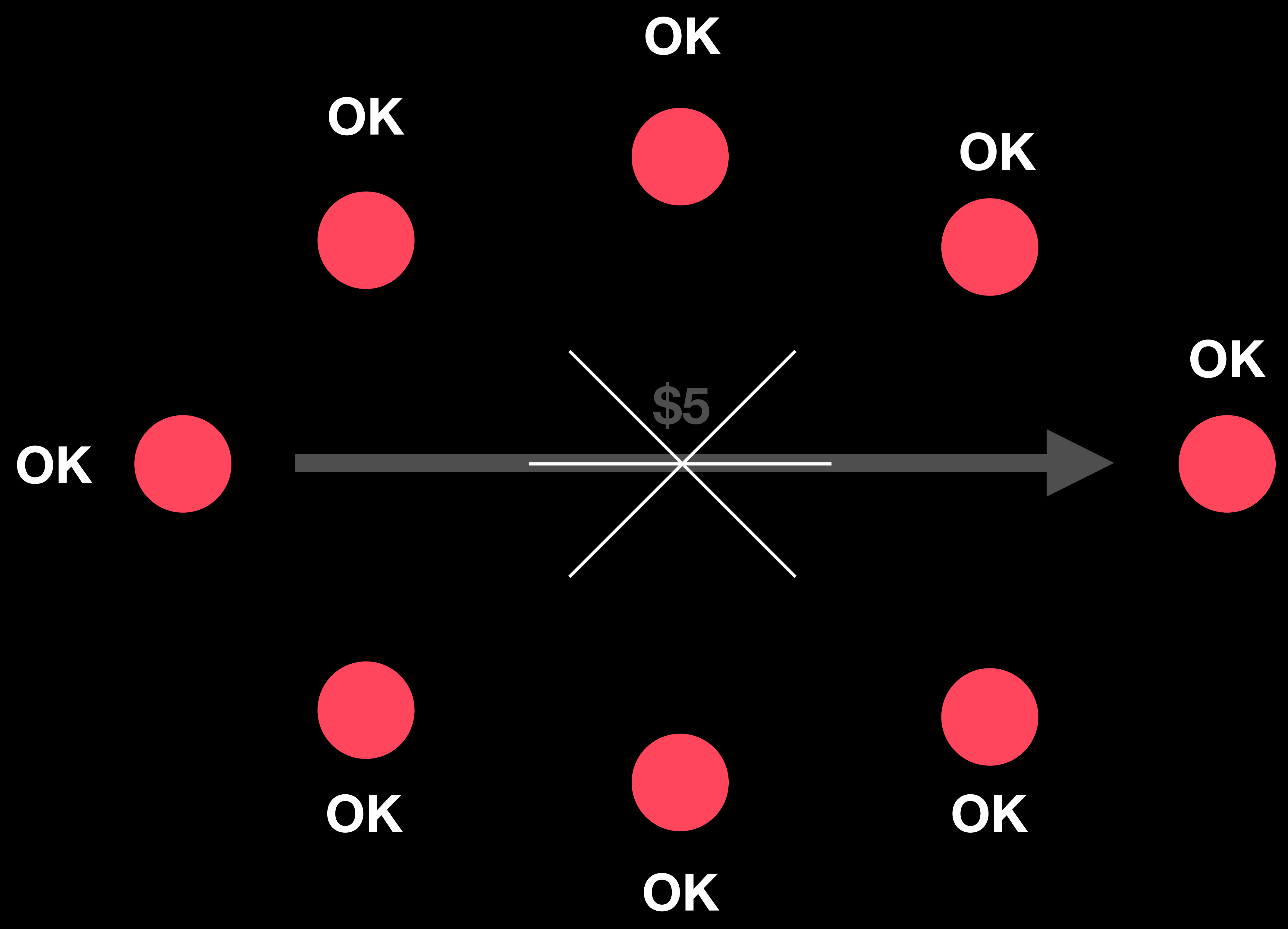
Digital Currency



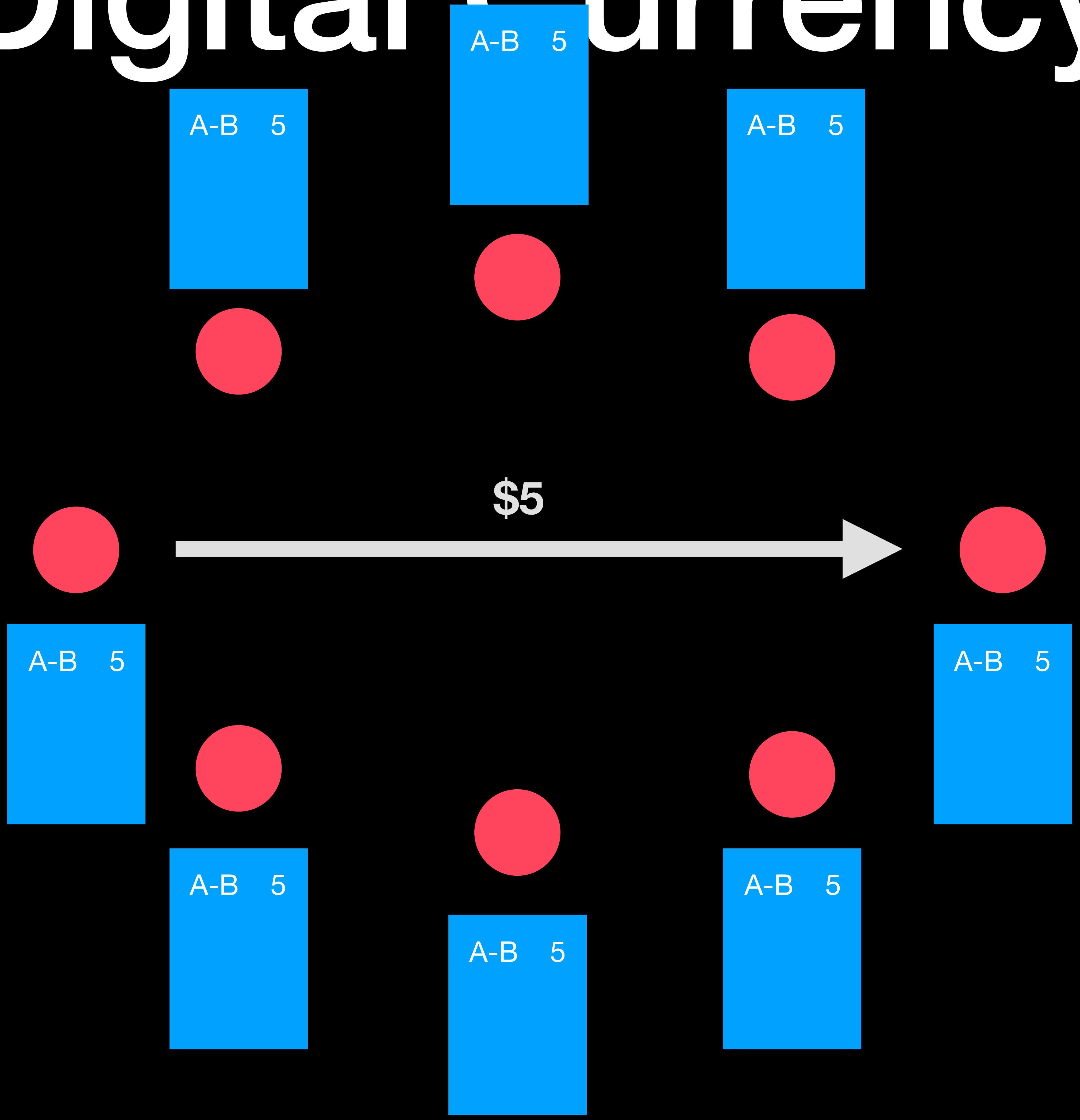
Digital Currency



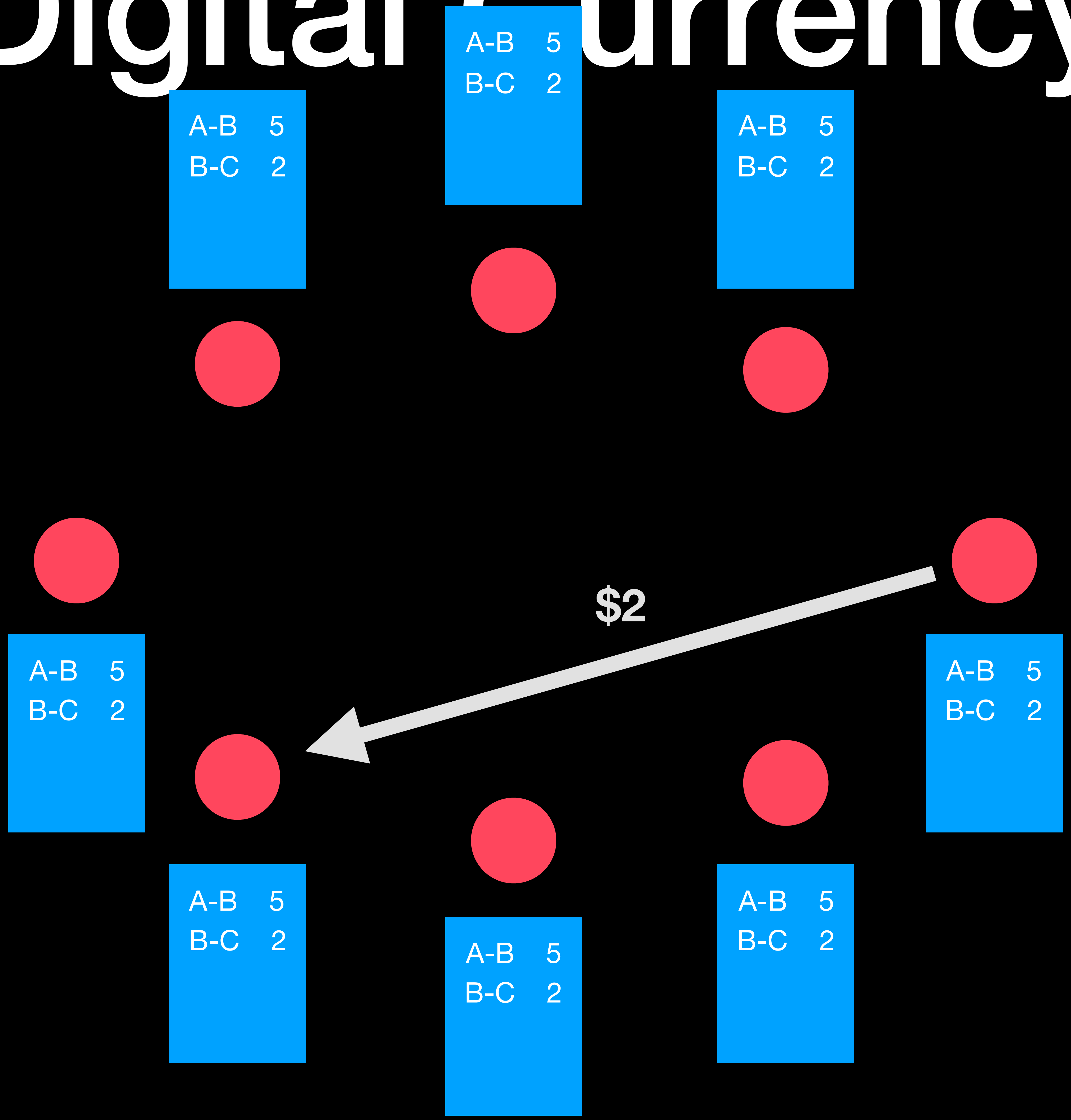
Digital Currency



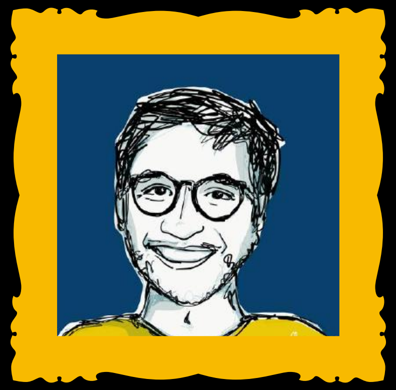
Digital Currency



Digital Currency



Naming



Local Naming

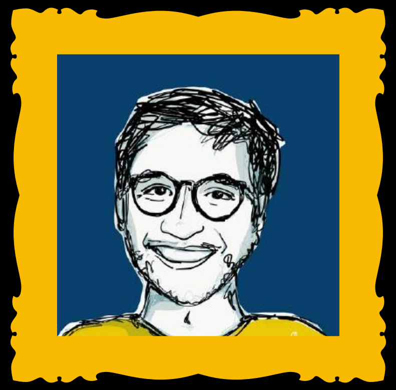
./nicola.jpg

Global Naming

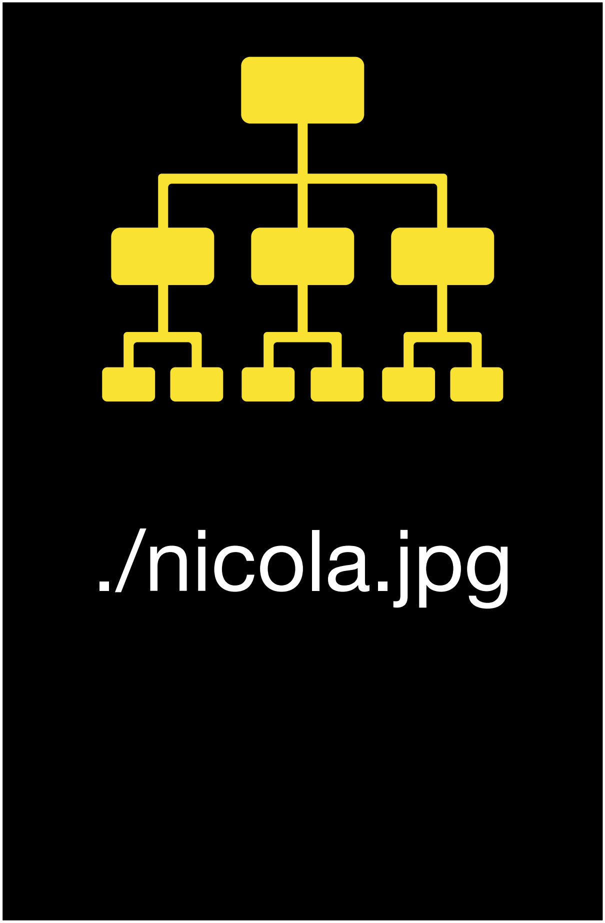
Trusted Party

[RFC1035]

Naming

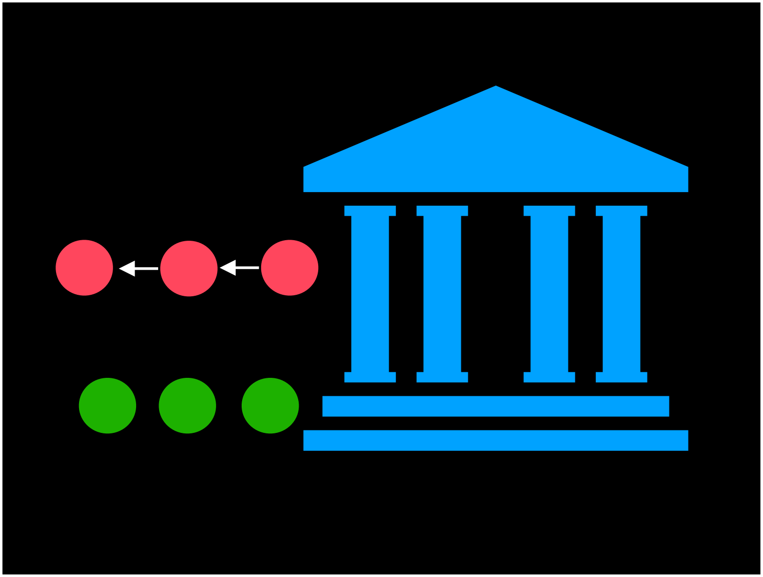


Local Naming



./nicola.jpg

Global Naming



Trusted Party

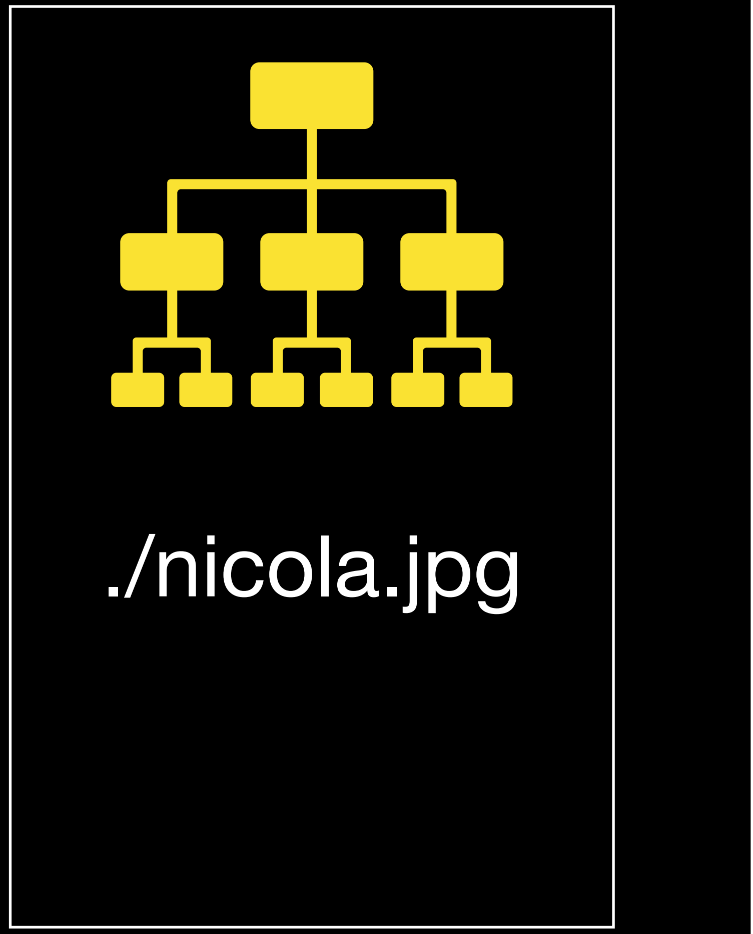
Untrusted Party

[RFC1035]

[RFC6962]
[CW2009]
[CONIKS]

Naming

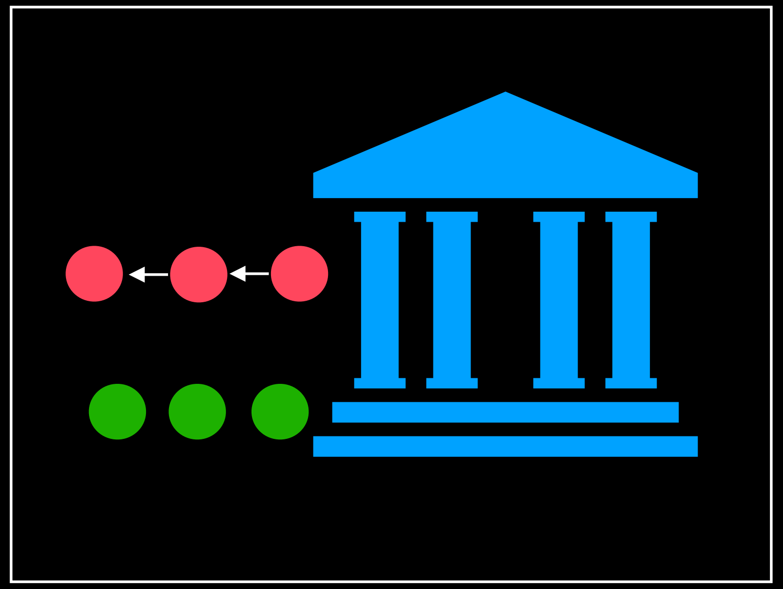
Local Naming



Global Naming

Trusted Party

[RFC1035]



Untrusted Party

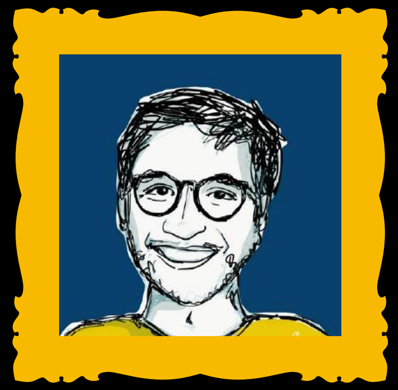
[RFC6962]
[CW2009]
[CONIKS]

hash( )
Qas13jdsjw

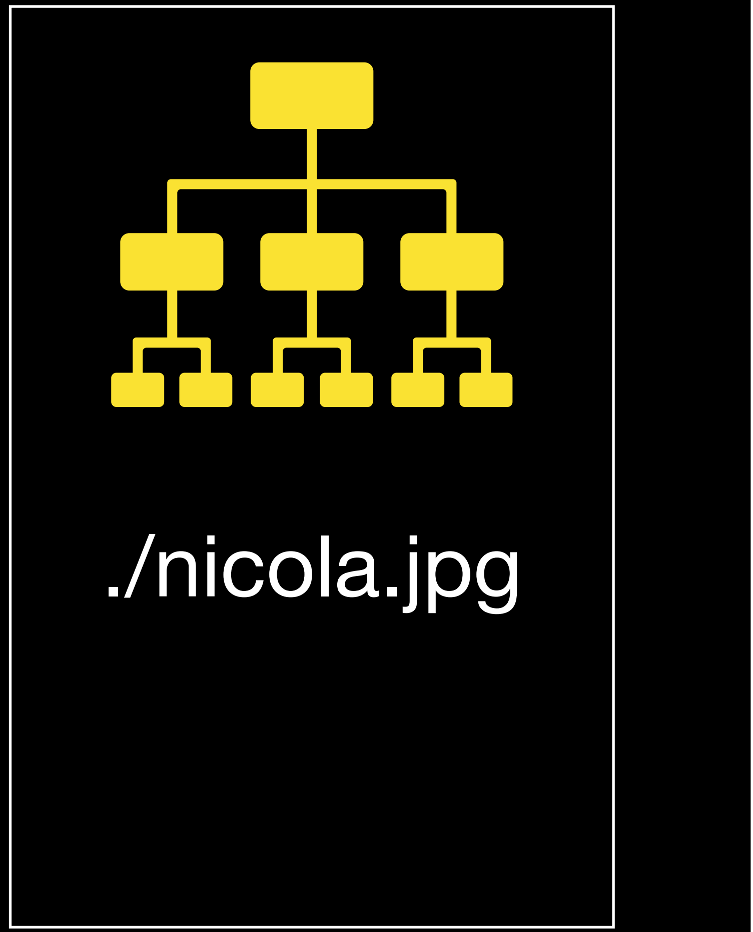
Cryptographic Hash

[RFC6920]
[BITTORRENT]
[IPFS]

Naming



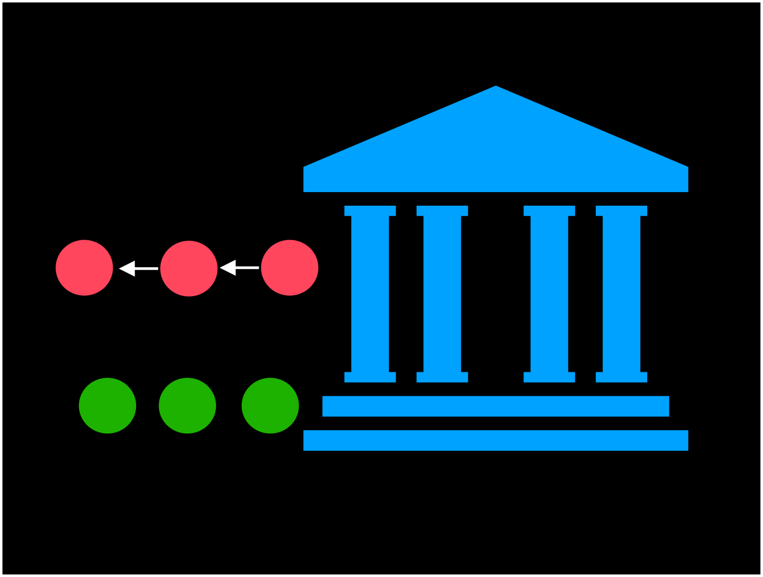
Local Naming



Global Naming

Trusted Party

[RFC1035]



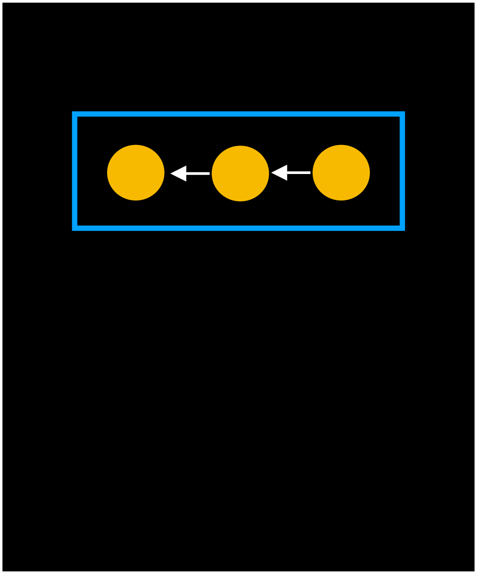
Untrusted Party

[RFC6962]
[CW2009]
[CONIKS]

hash( )
Qas13jdsjw

Cryptographic Hash

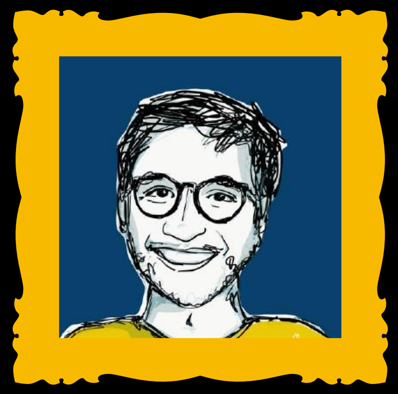
[RFC6920]
[BITTORRENT]
[IPFS]

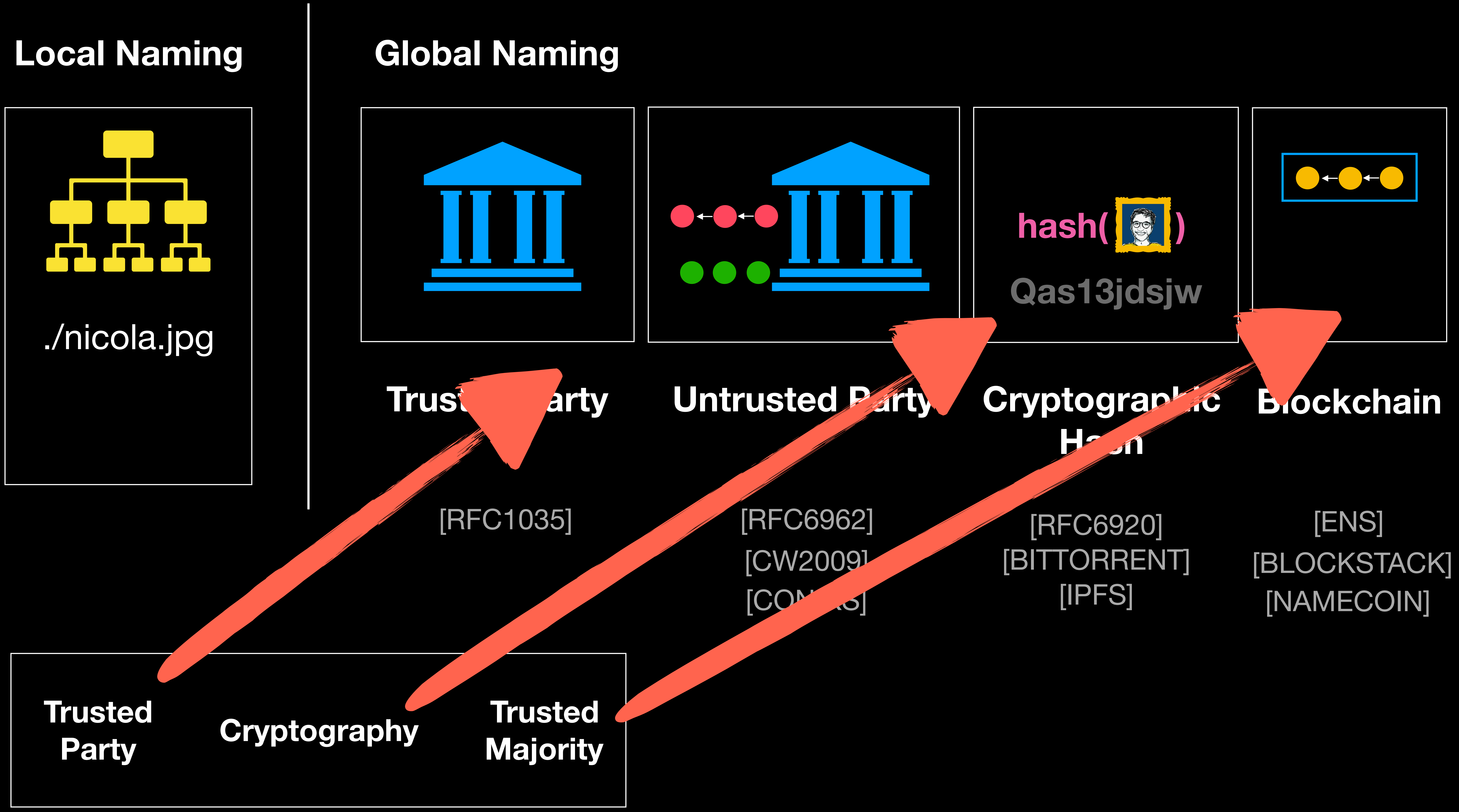


Blockchain

[ENS]
[BLOCKSTACK]
[NAMECOIN]

Naming





Local Naming

./nicola.jpg

Global Naming

Trusted Party

[RFC1035]

Untrusted Party

[RFC6962]
[CW2009]
[CONIKS]

Cryptographic Hash

[RFC6920]
[BITTORRENT]
[IPFS]

Blockchain

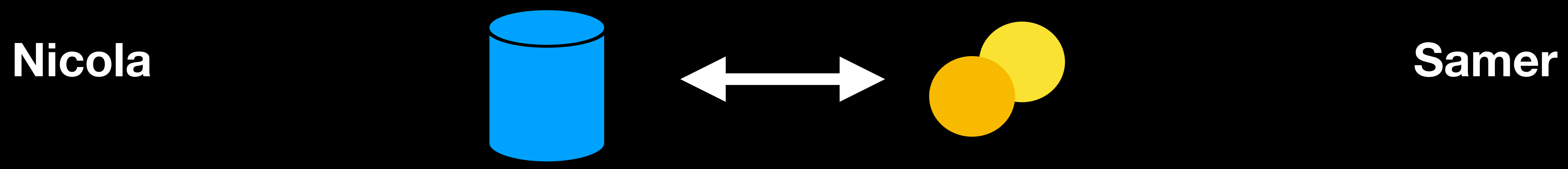
[ENS]
[BLOCKSTACK]
[NAMECOIN]

Trusted Party

Cryptography

Trusted Majority

Fair Exchange of Services



Nicola

Samer

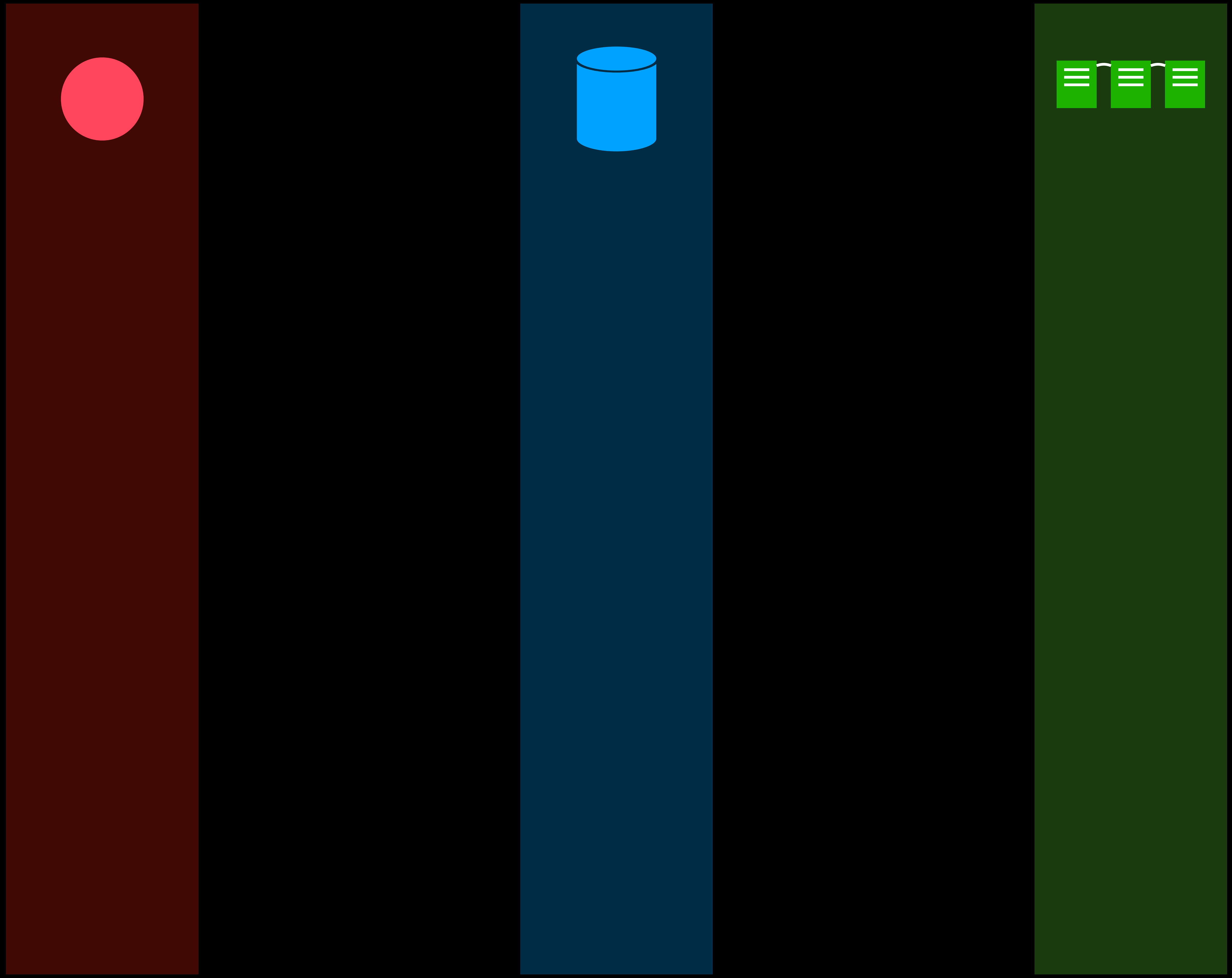
Fairness Either both parties receive their inputs or none

Timeliness Exchange either happens or does terminate

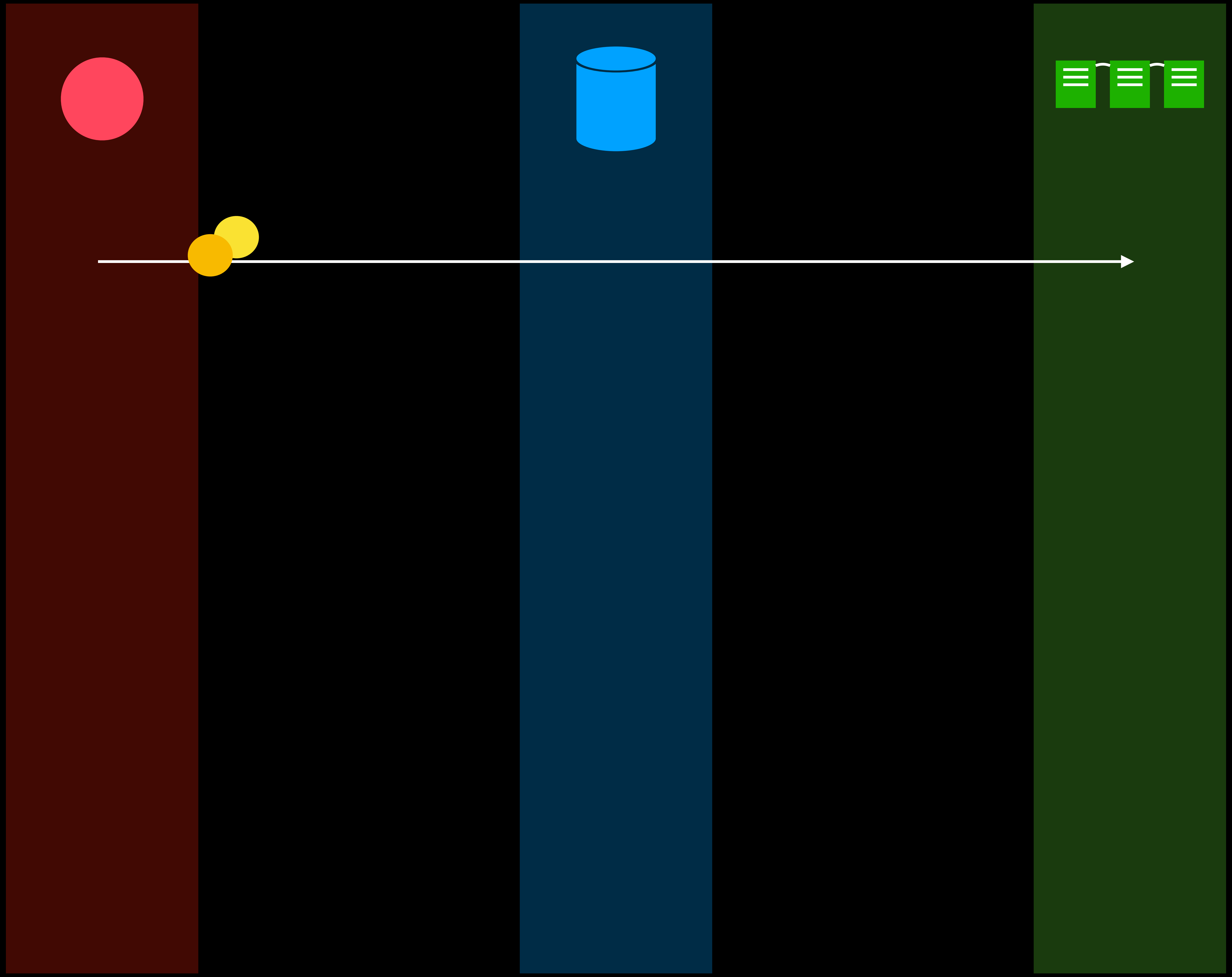
Completeness If seller is honest, both parties receive their inputs

Soundness

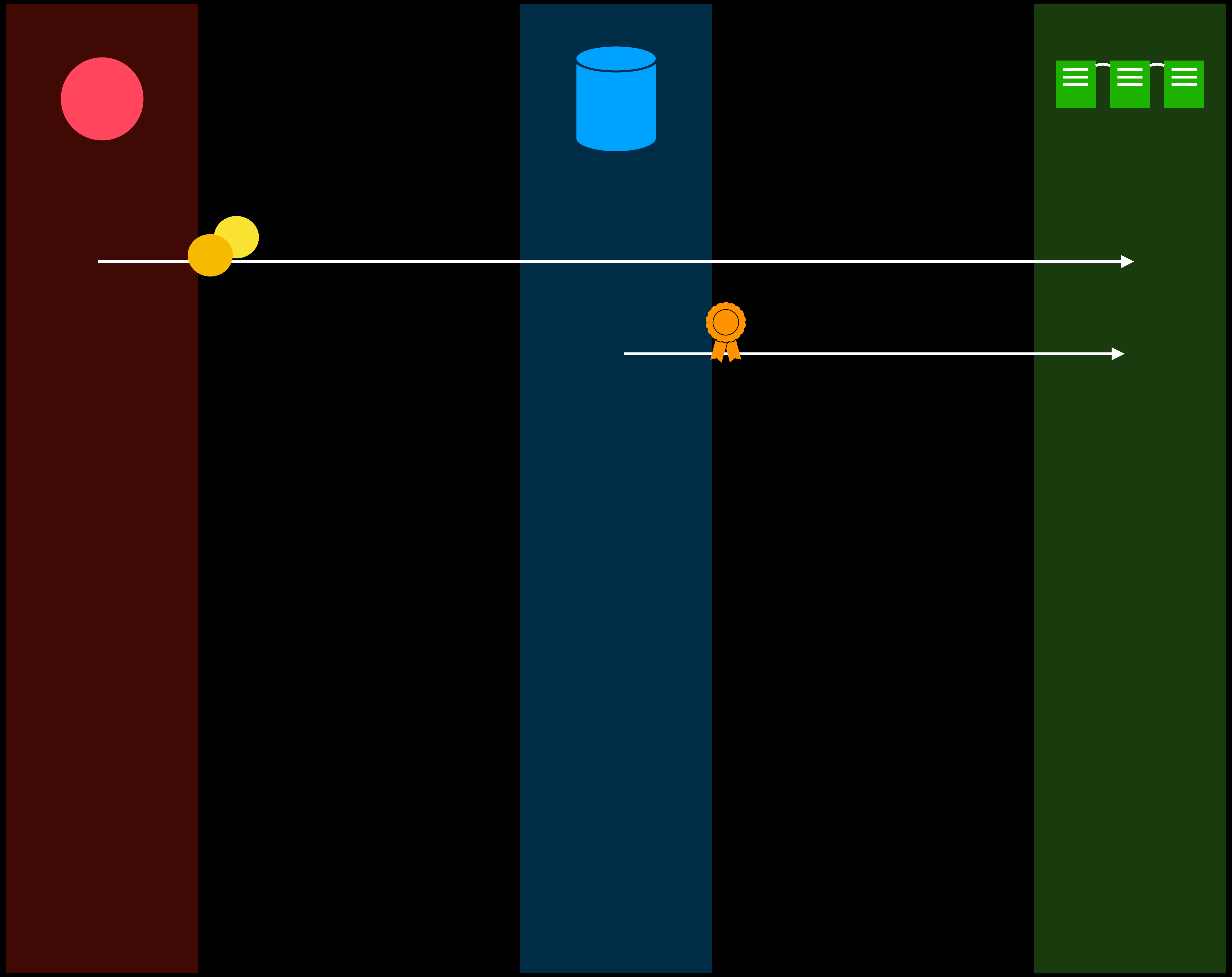
Fair Exchange of Services



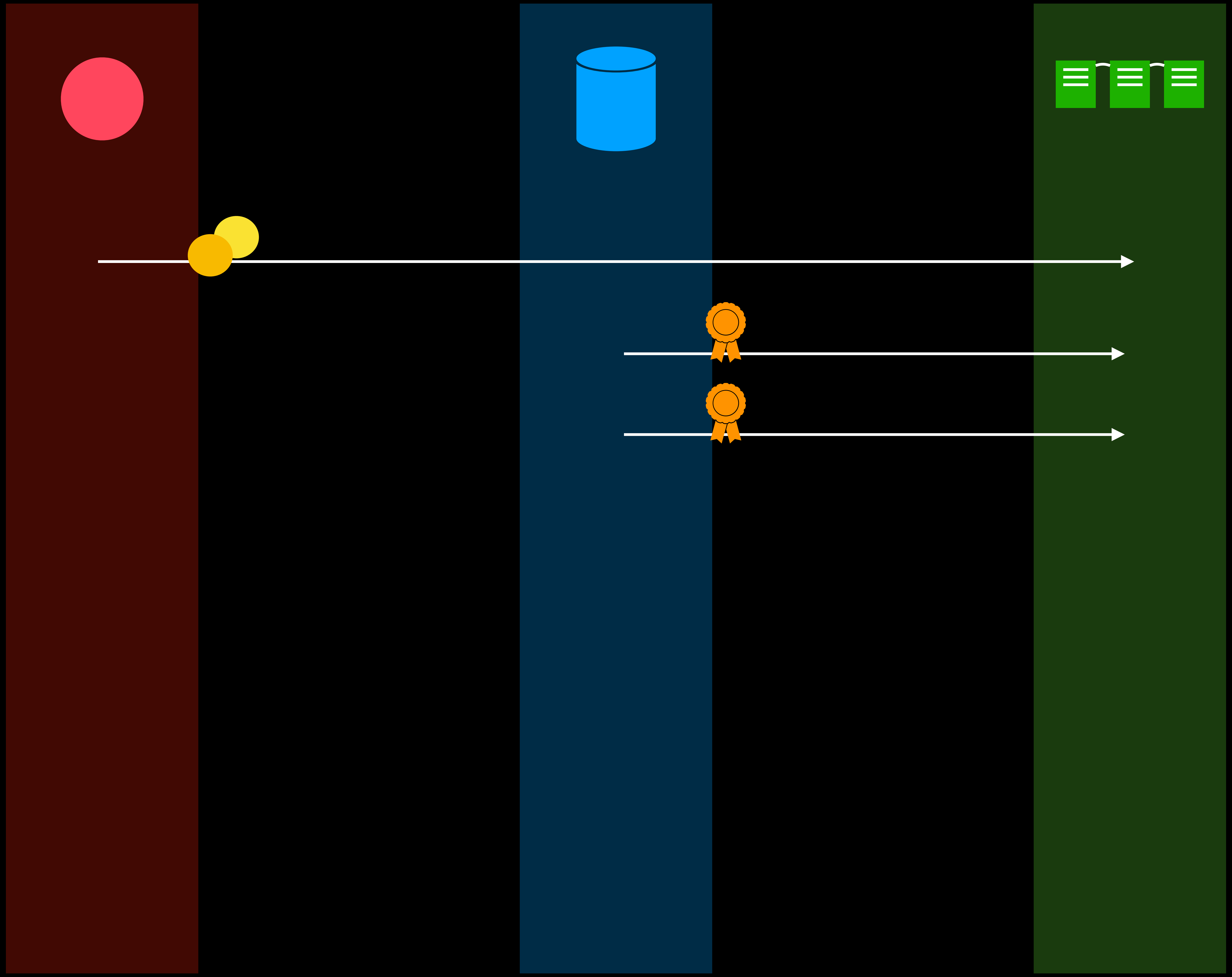
Fair Exchange of Services



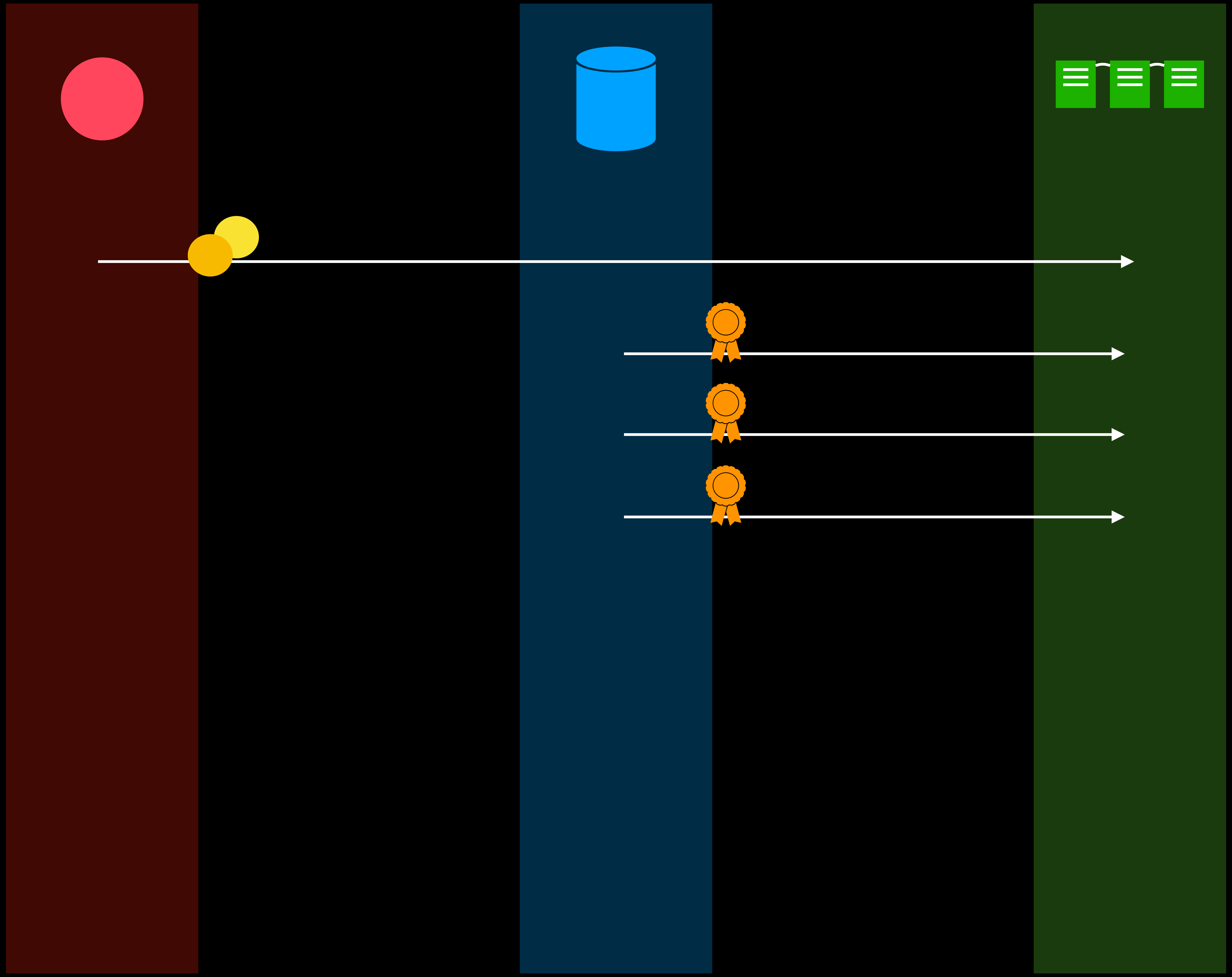
Fair Exchange of Services



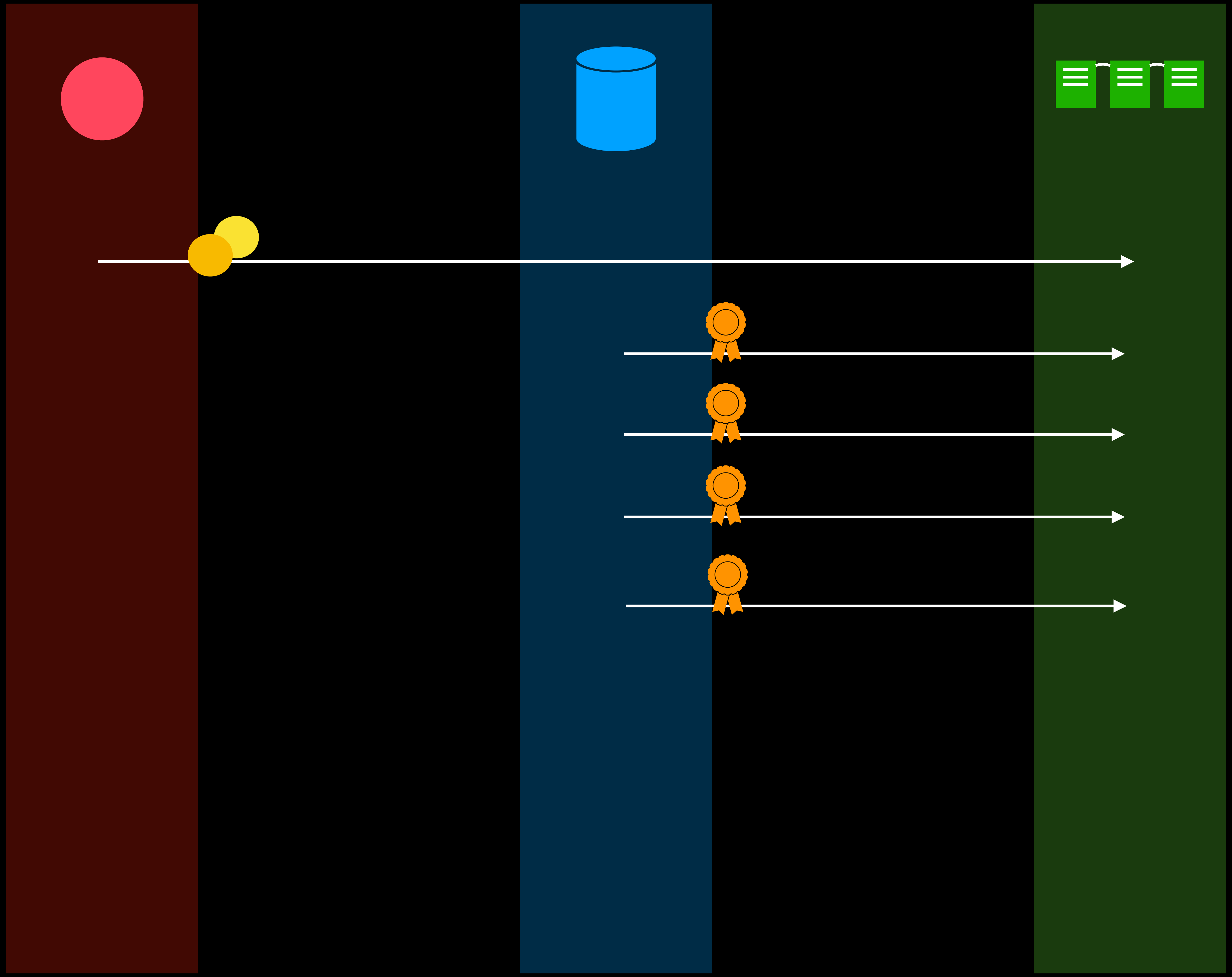
Fair Exchange of Services



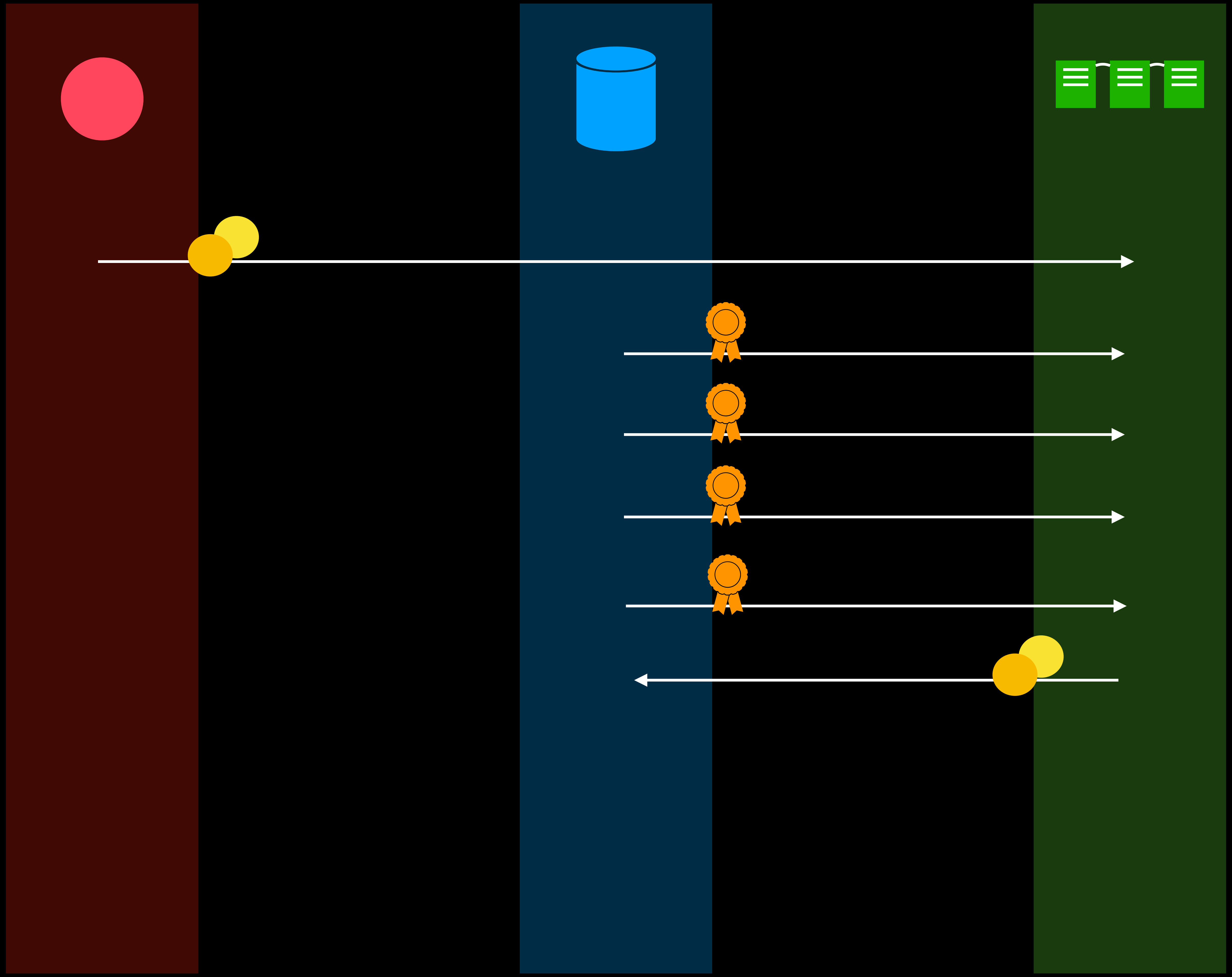
Fair Exchange of Services



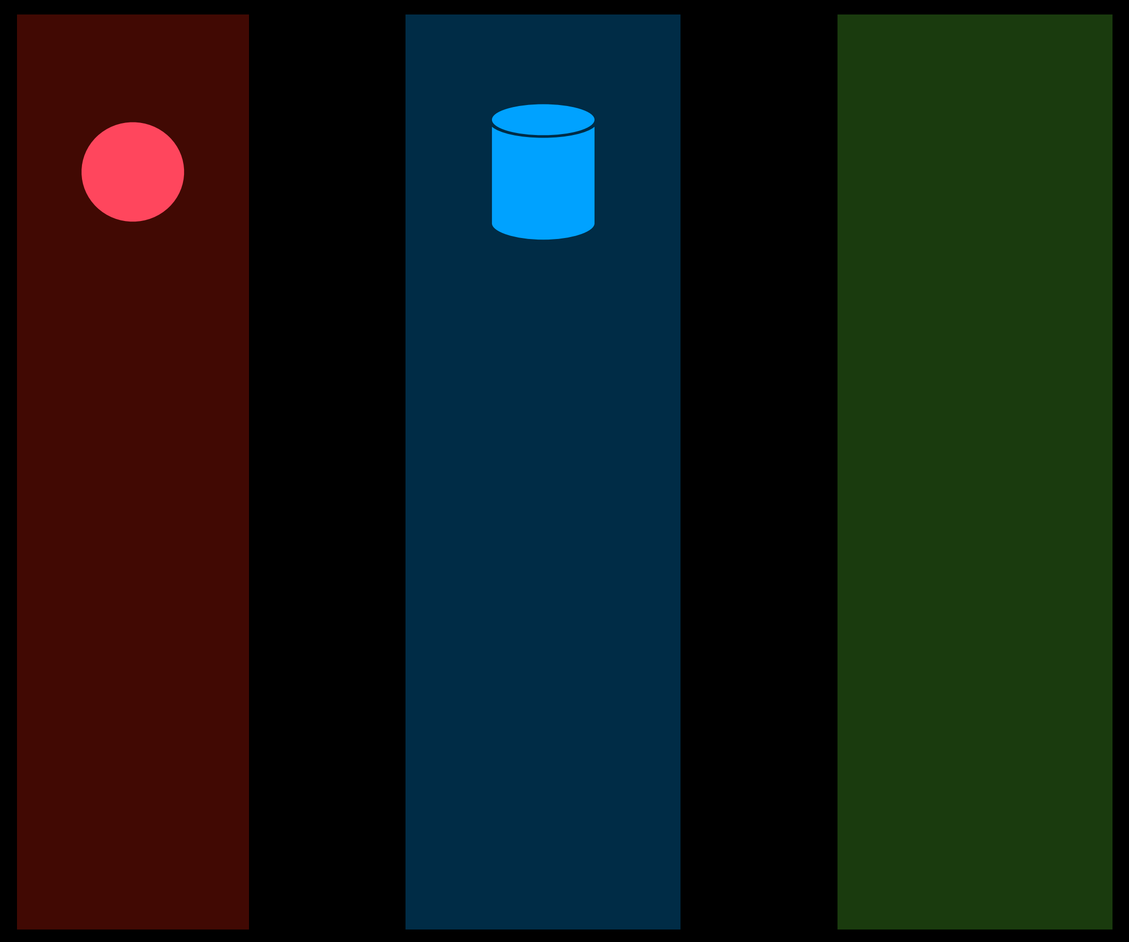
Fair Exchange of Services



Fair Exchange of Services



Fair Exchange of Services



[NICOLA's MASTER]
[ZKCSP]
[ZKCP]
…

Trusted Party

Trusted Hardware

Trusted Majority

Any Trust

Trusted Auditors

Reputation

Rewards

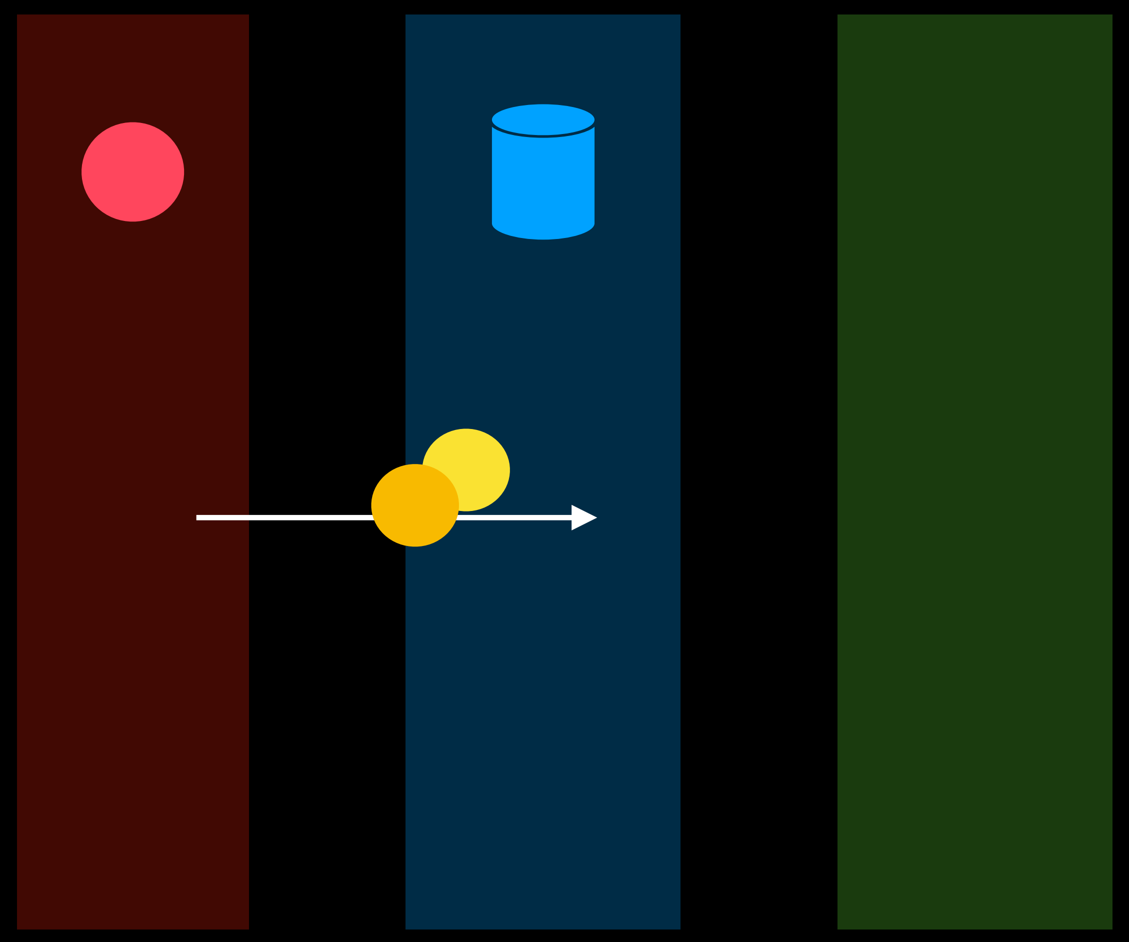
Penalizations

Sigma Protocols

SNARKs

…

Fair Exchange of Services



[NICOLA's MASTER]
[ZKCSP]
[ZKCP]
…

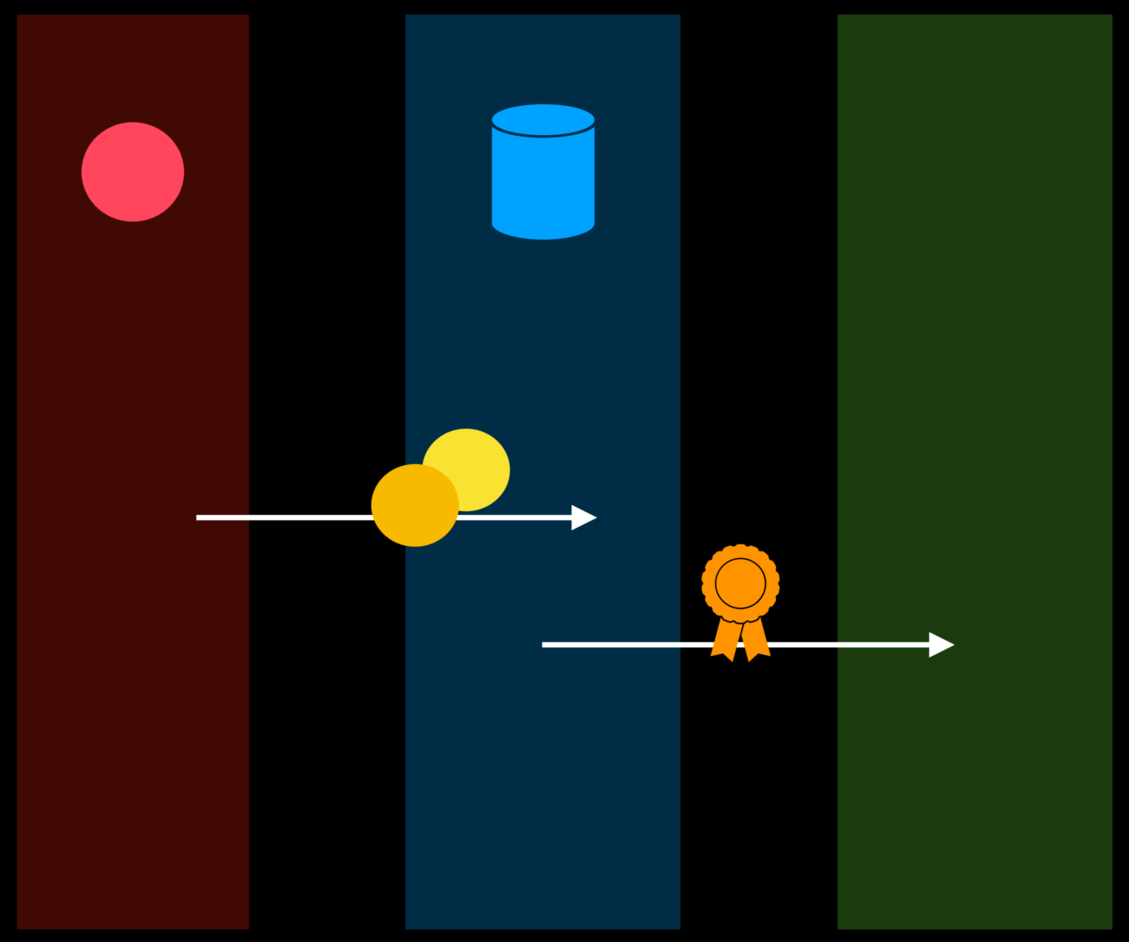
Trusted Party   Trusted Hardware   Trusted Majority   Any Trust

Trusted Auditors   Reputation

Rewards   Penalizations

Sigma Protocols   SNARKs   …

Fair Exchange of Services



Trusted Party
Trusted Hardware
Trusted Majority
Any Trust

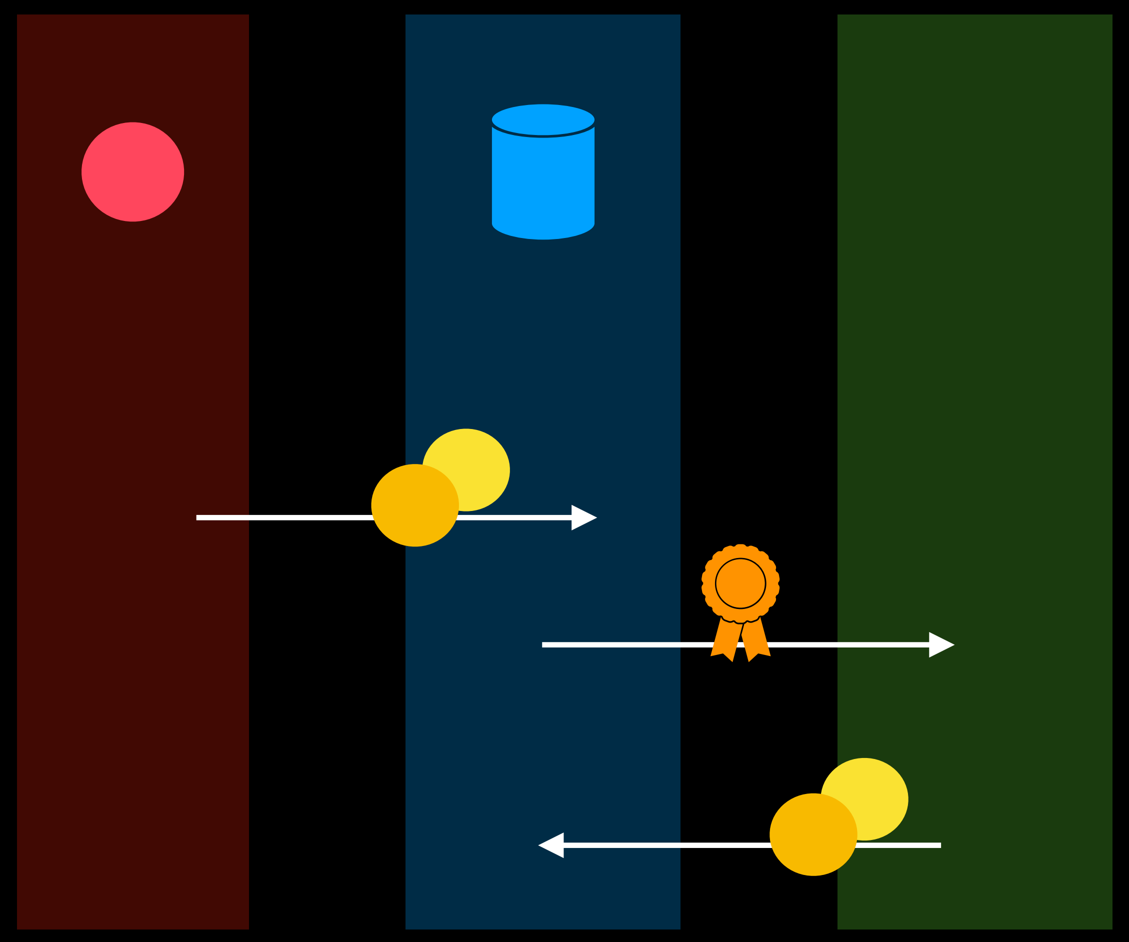
Trusted Auditors
Reputation

Rewards
Penalizations

Sigma Protocols
SNARKs
...

[NICOLA's MASTER]
[ZKCSP]
[ZKCP]
...

Fair Exchange of Services



Trusted Party · Trusted Hardware · Trusted Majority · Any Trust

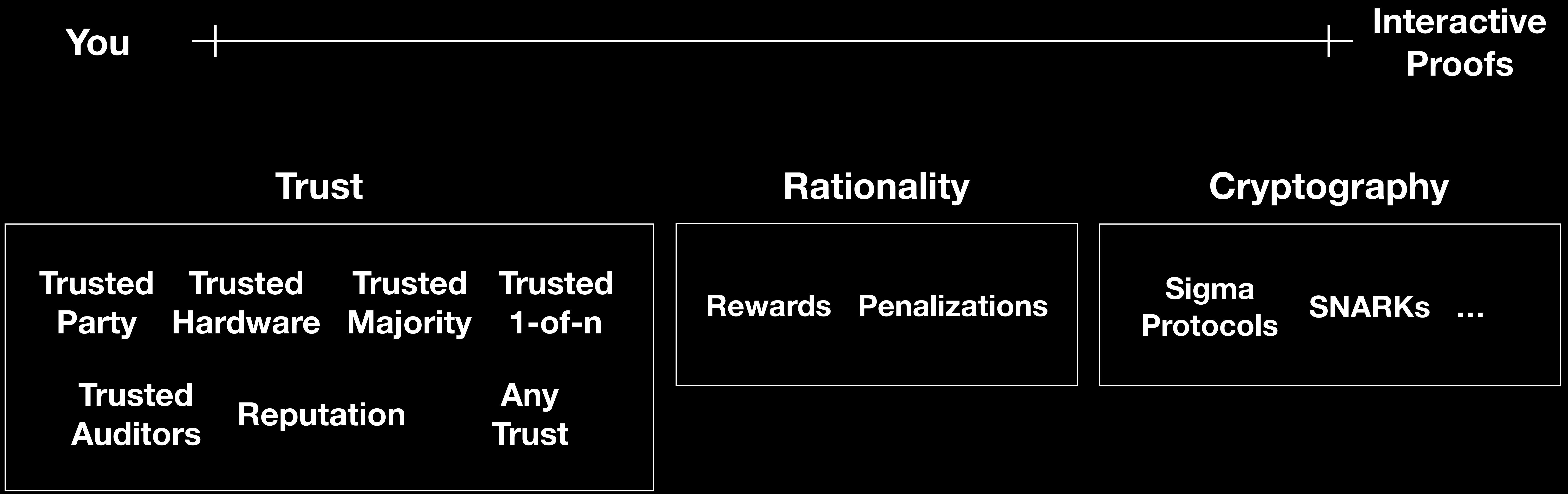
Trusted Auditors · Reputation

Rewards · Penalizations

Sigma Protocols · SNARKs · …

[NICOLA's MASTER]
[ZKCSP]
[ZKCP]
…

Trust Spectrum



You

Interactive Proofs

Trust

Trusted Party

Trusted Hardware

Trusted Majority

Trusted 1-of-n

Trusted Auditors

Reputation

Any Trust

Rationality

Rewards

Penalizations

Cryptography

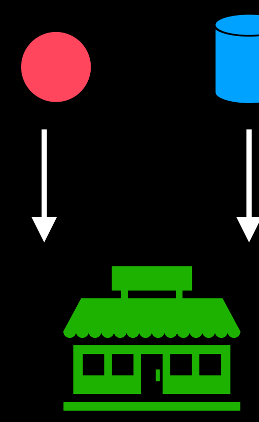
Sigma Protocols

SNARKs

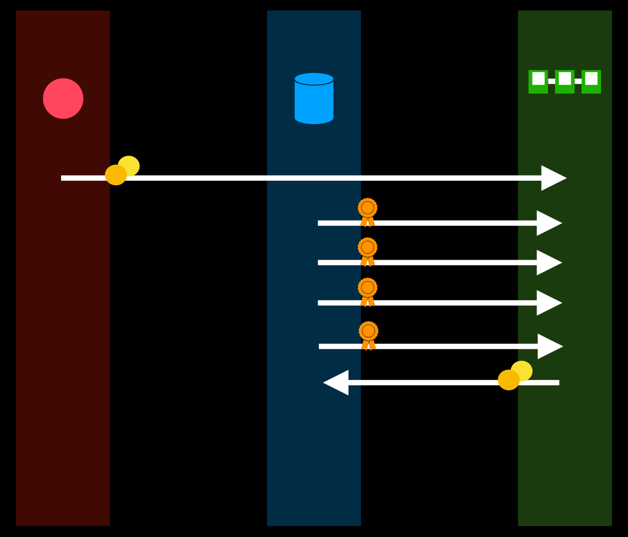
...

Verifiable Markets

Order matching

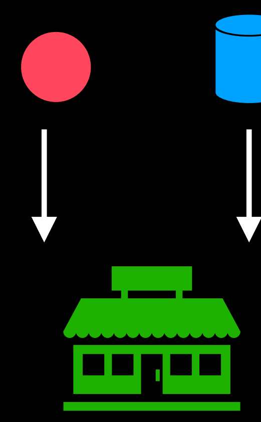


Settlement

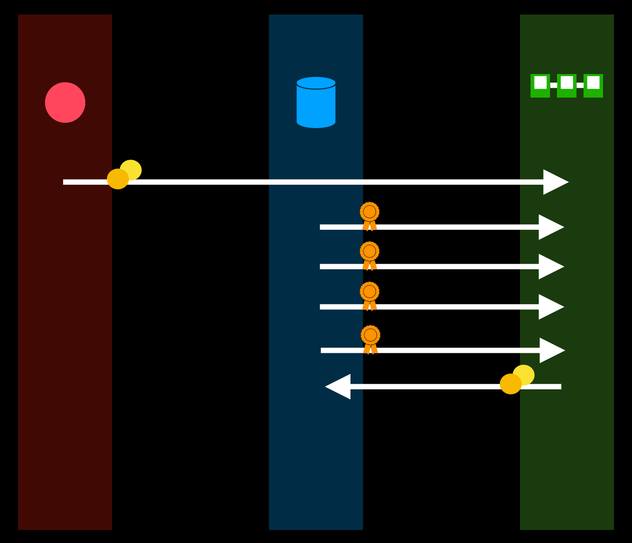


Verifiable Markets

Order matching



Settlement

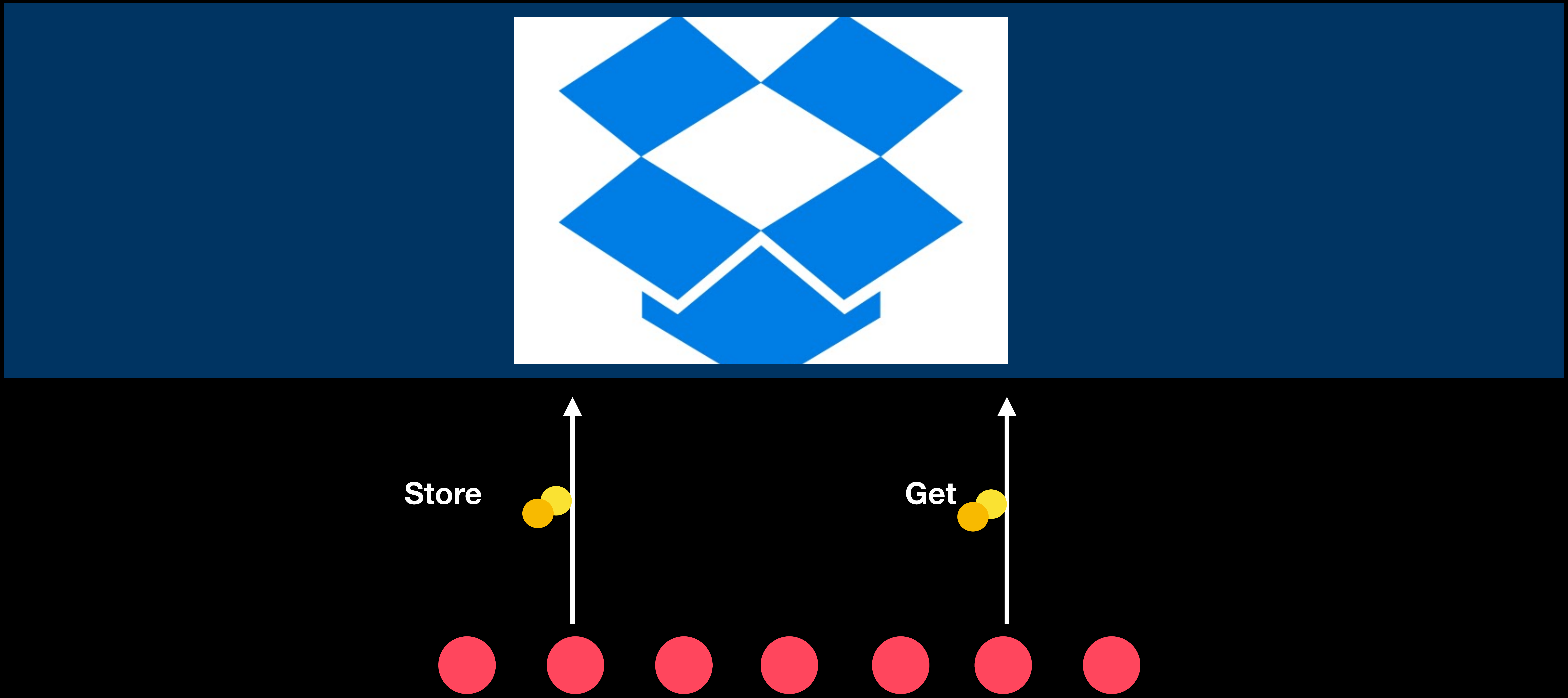


- Don’t need to trust individual service provider
- Anyone can participate in the market as participant

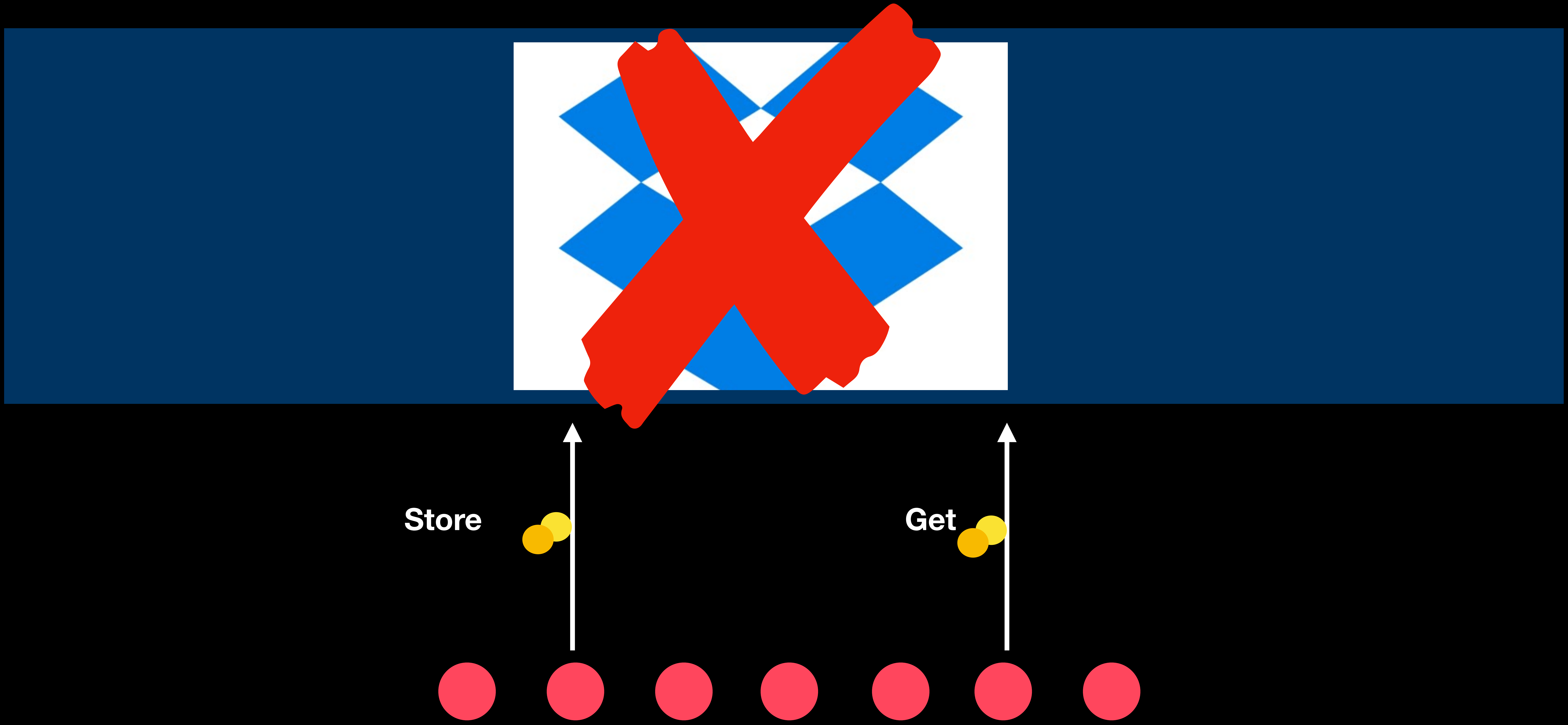
Part 3

Filecoin (abstract)

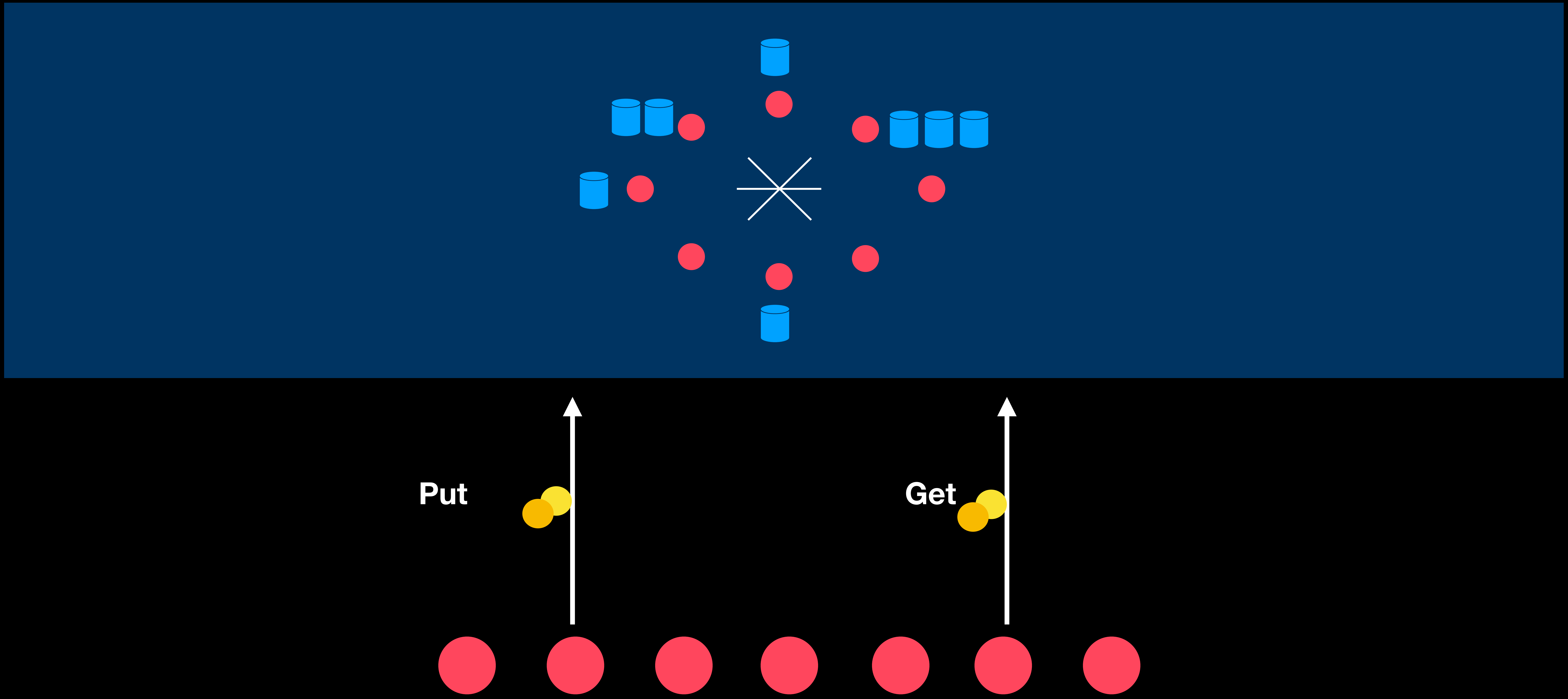
Cloud Storage



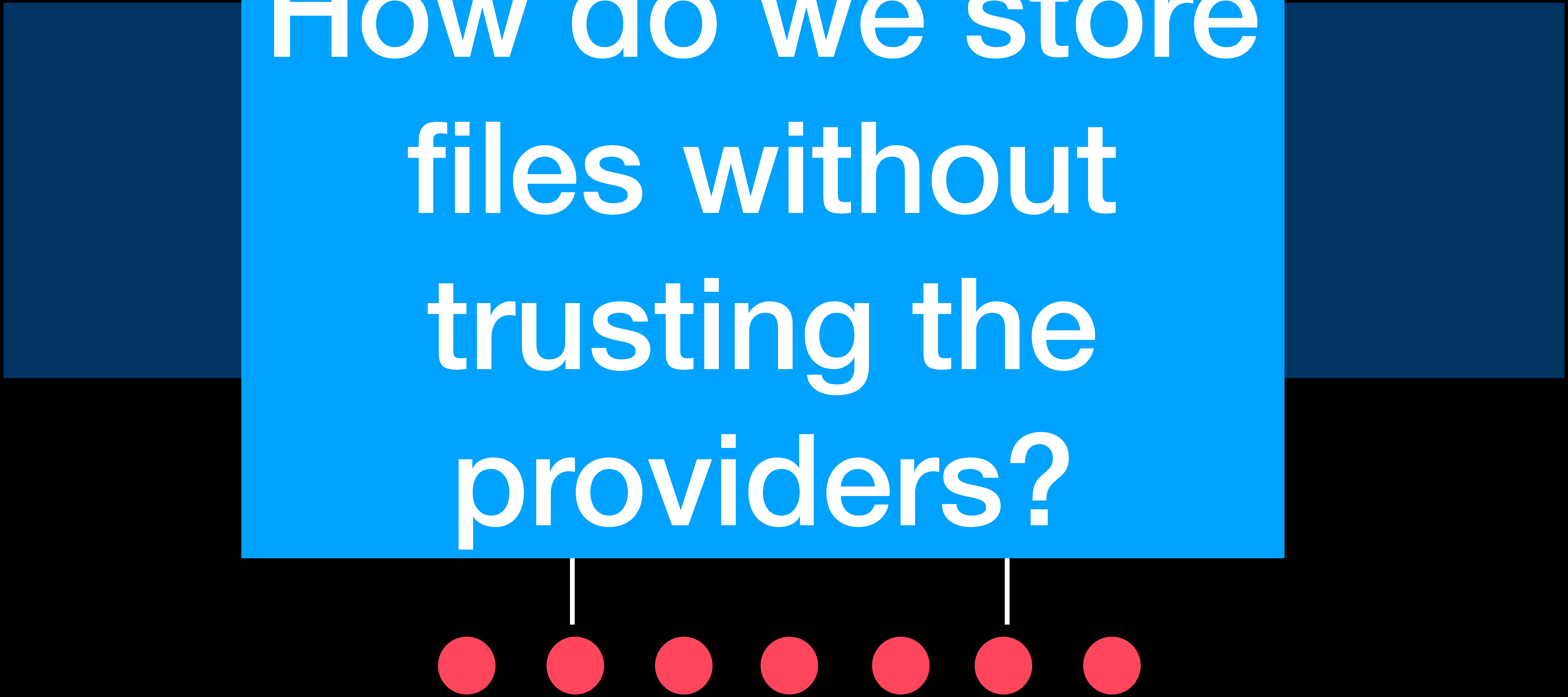
Cloud Storage



Decentralized Storage



Decentralized Storage

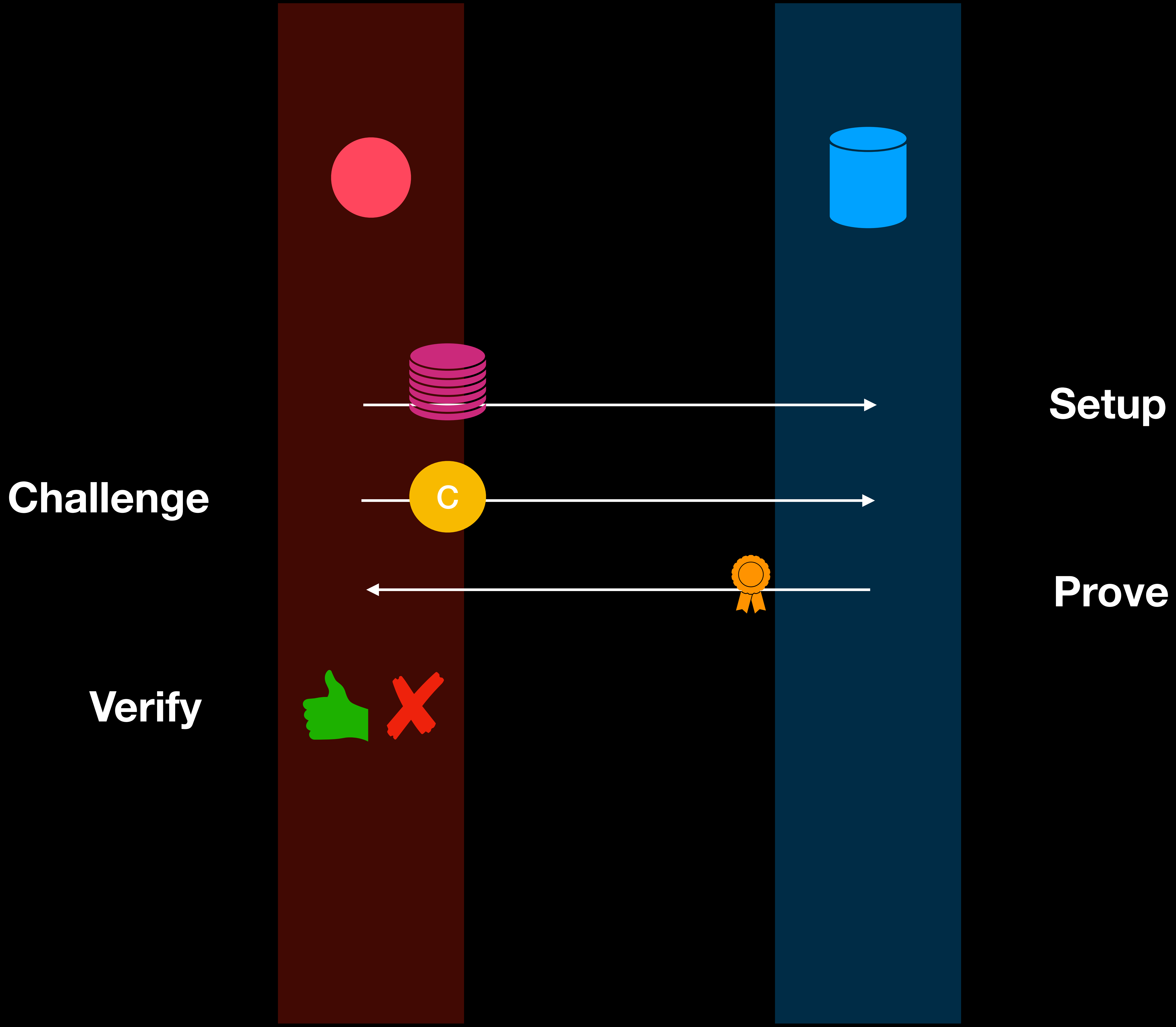


How do we store files without trusting the providers?

Filecoin Protocol

Get - Retrieve a file
Put - Store a file
Pledge - Add storage

Proofs of Storage



Proofs of Storage

Complete everyone with storage will generate valid proofs

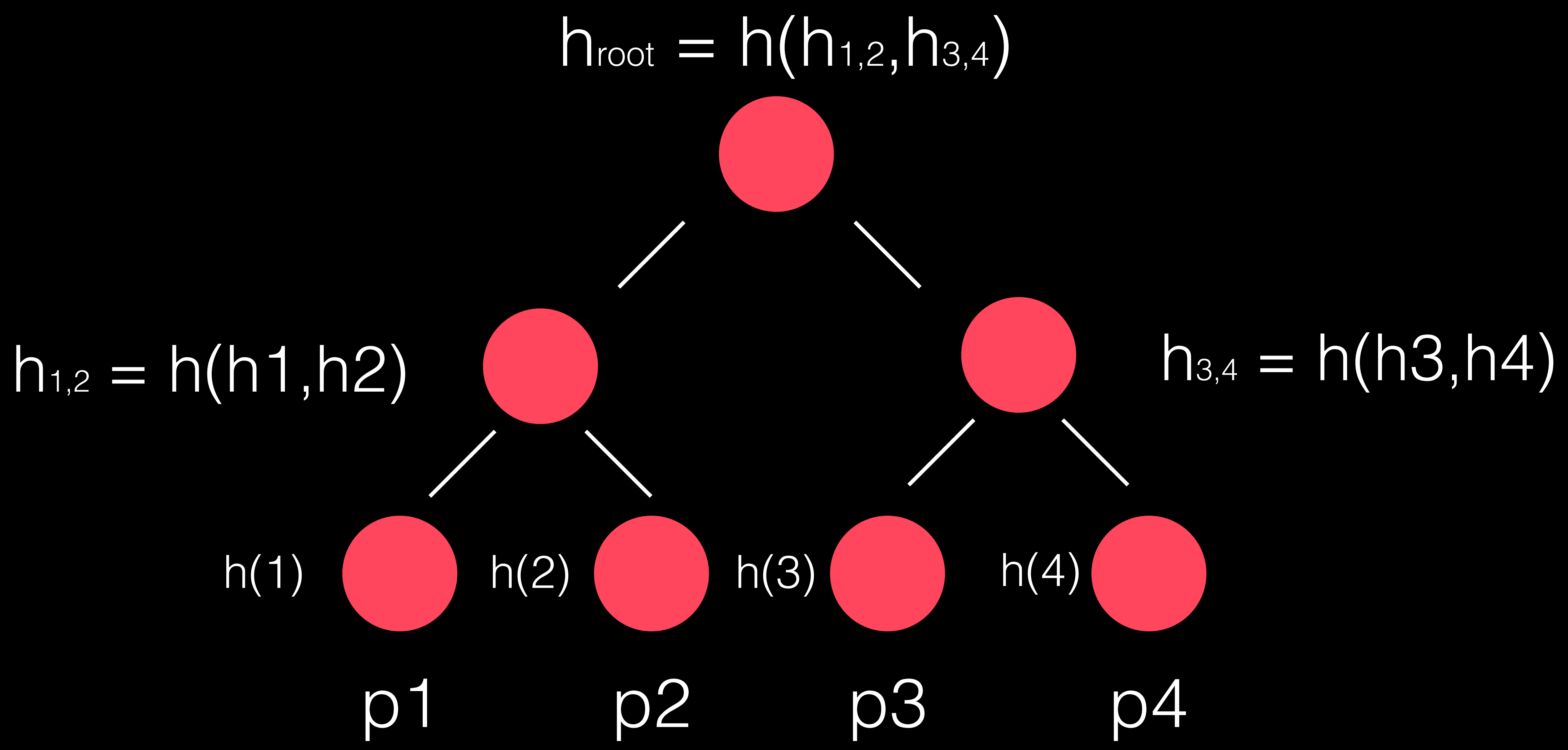
Sound no adversary can generate fake proofs

Public Verifiable everyone can verify proofs

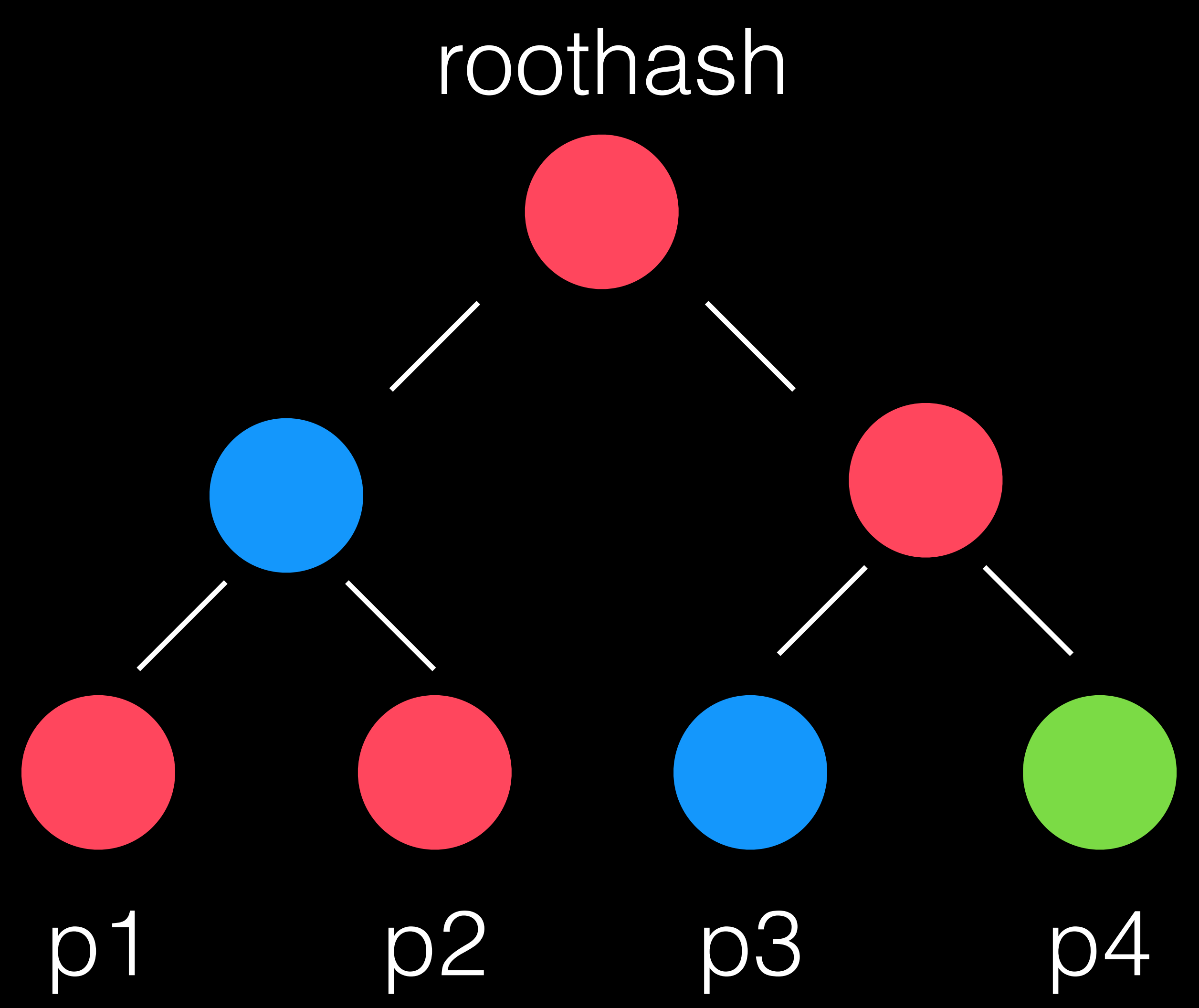
Transparent there is no secret information that can generate proofs info

Useful proofs are about useful storage

Proofs of Storage



Proofs of Storage



Proof of Replication

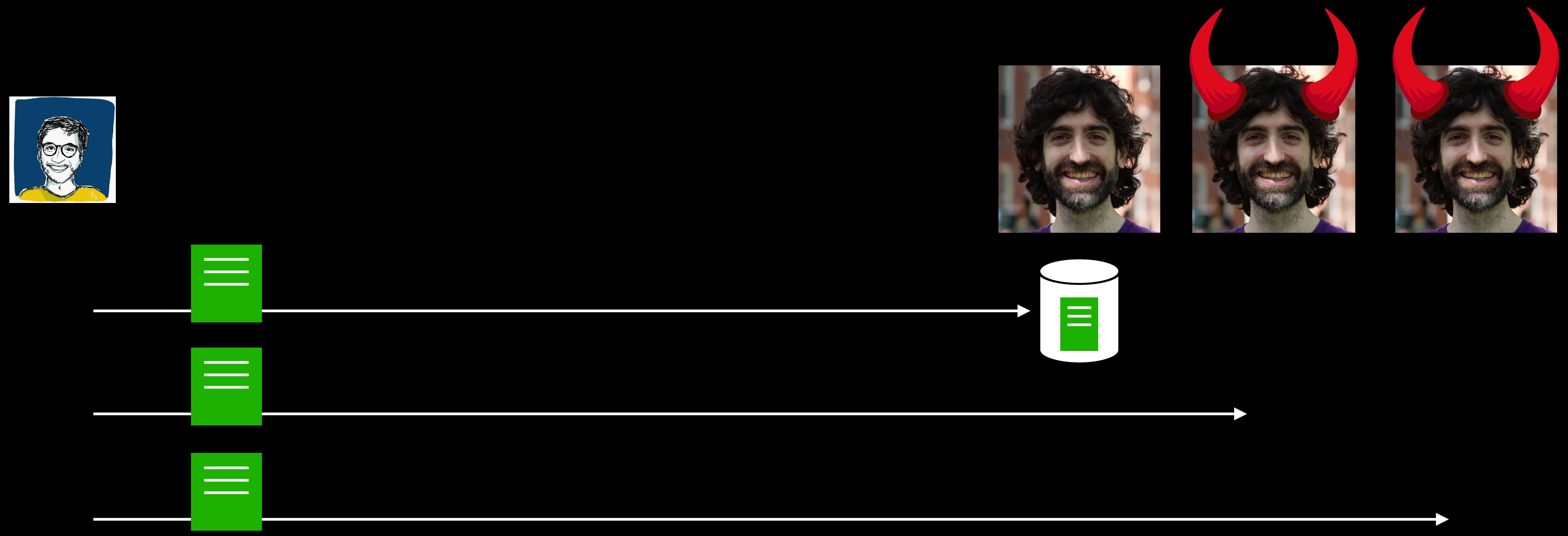
Sybil attack

Outsourcing attack

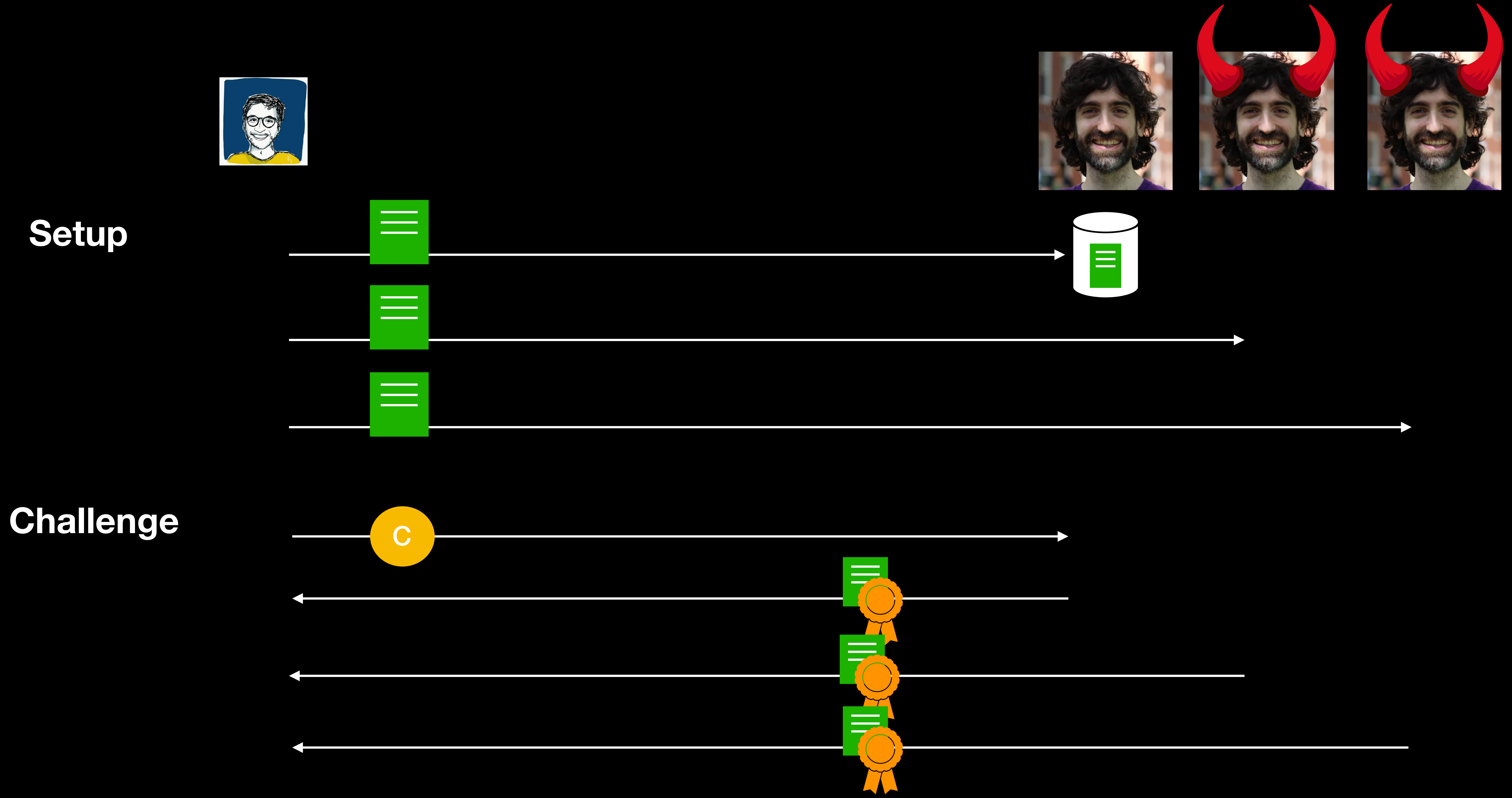
Generation attack

Proof of Retrievability

Setup



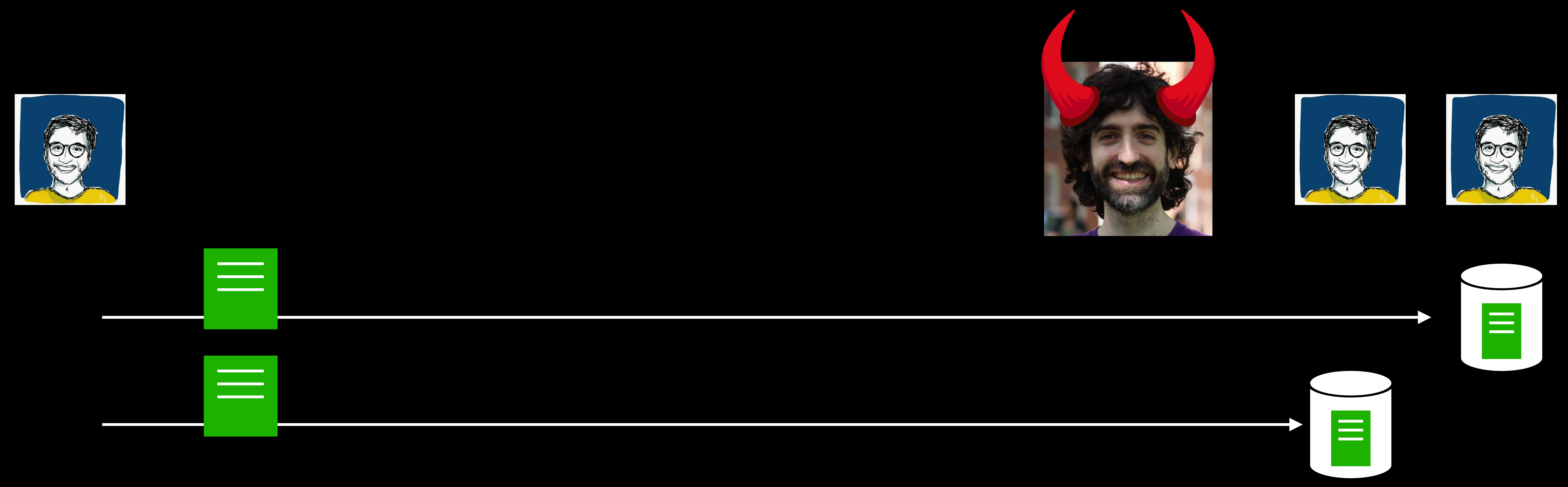
Proof of Retrievability



Setup

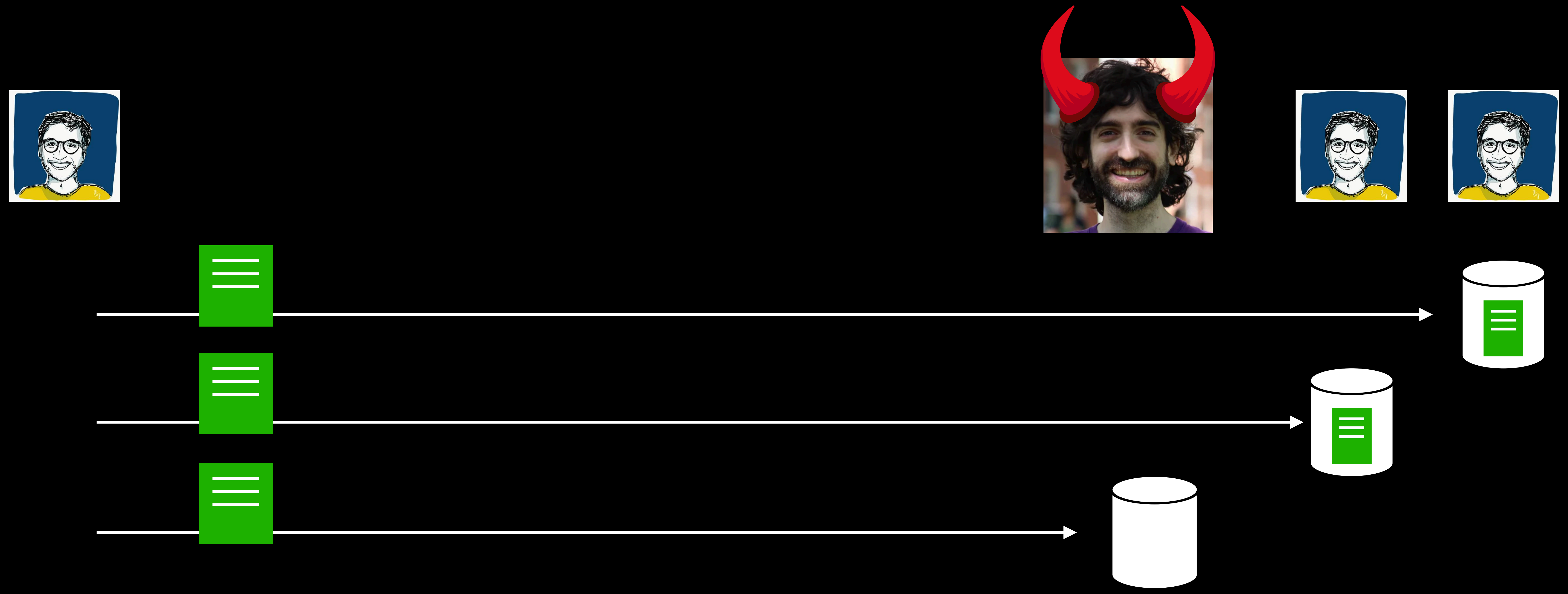
Challenge

Proof of Retrievability



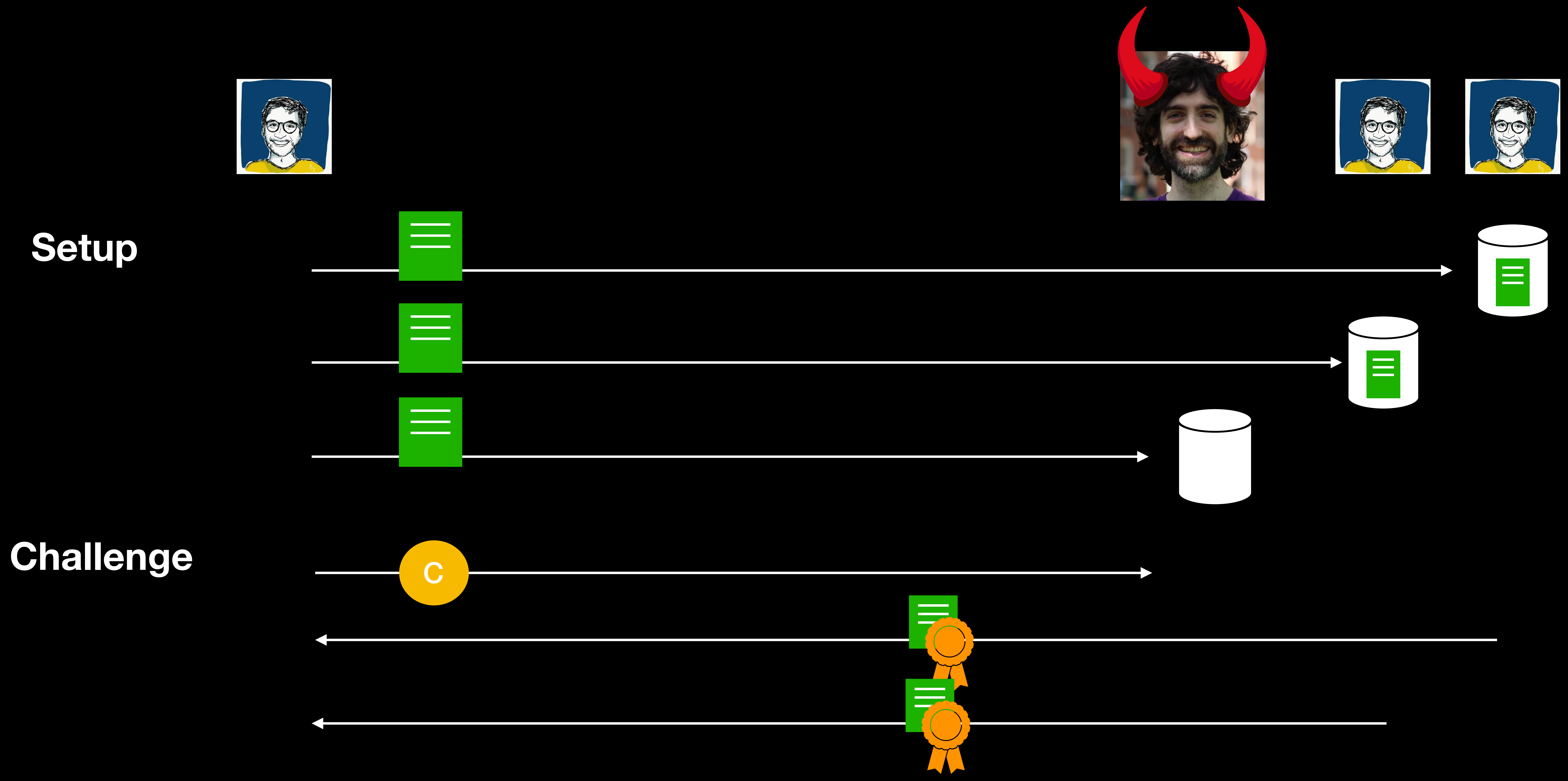
Setup

Proof of Retrievability



Setup

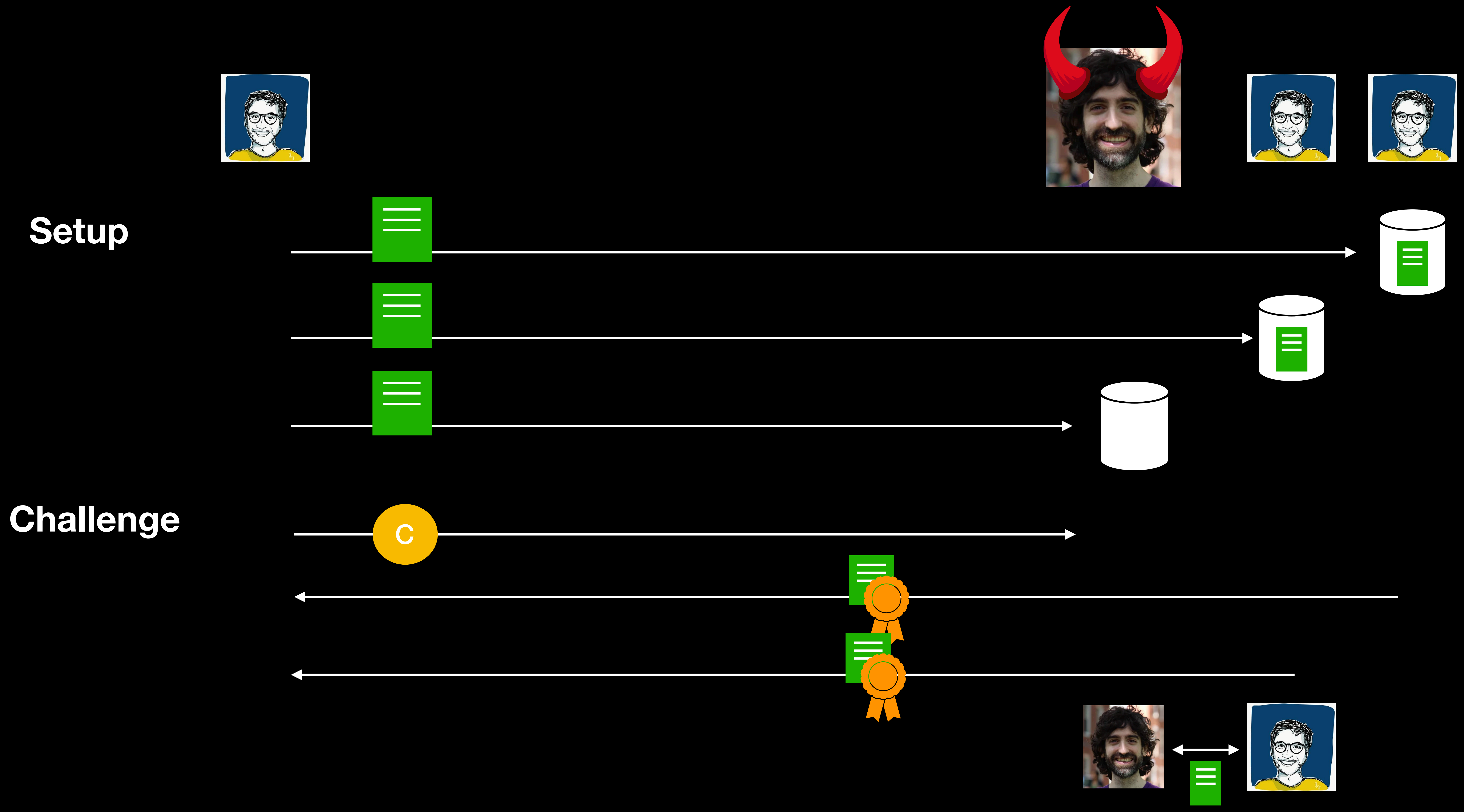
Proof of Retrievability



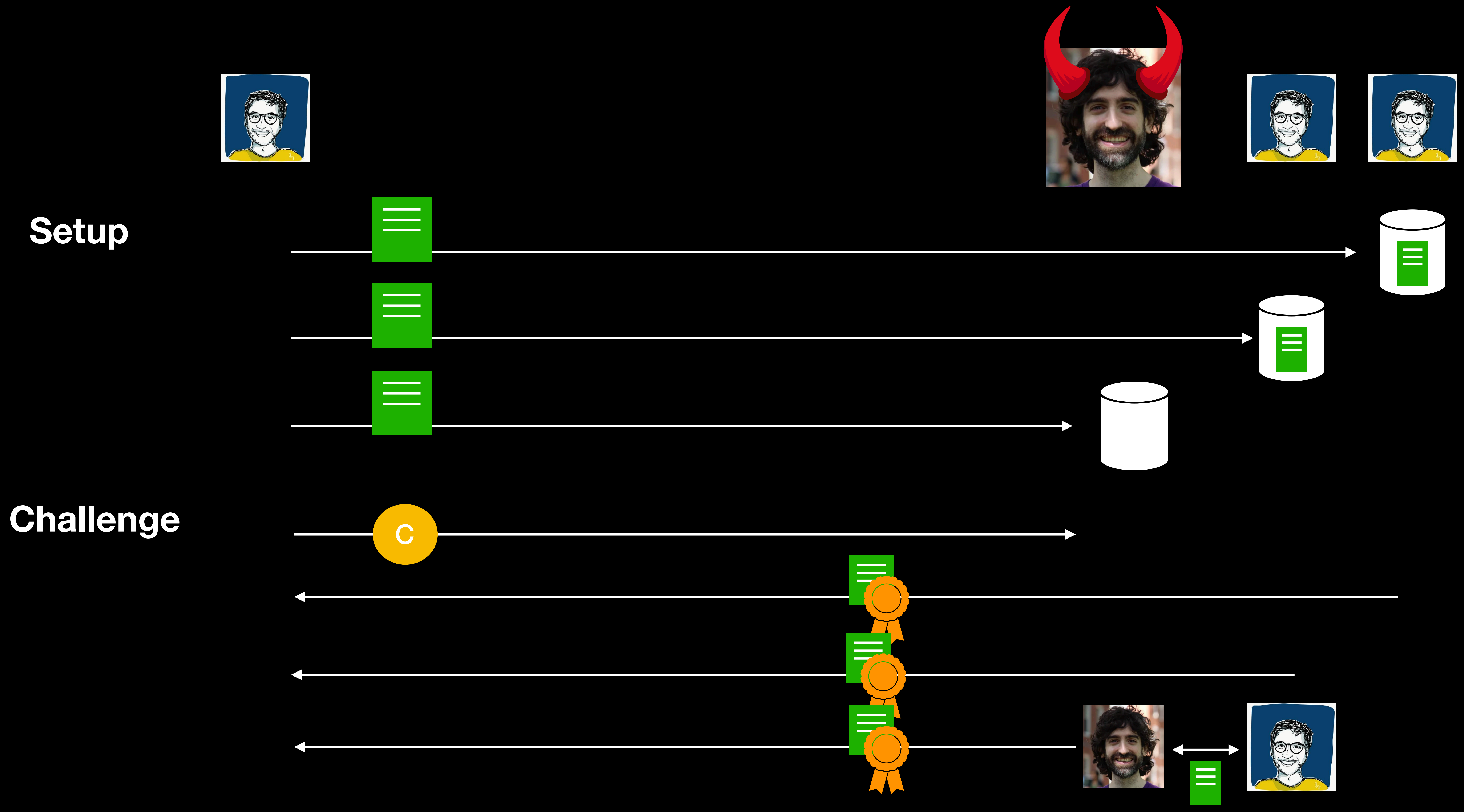
Setup

Challenge

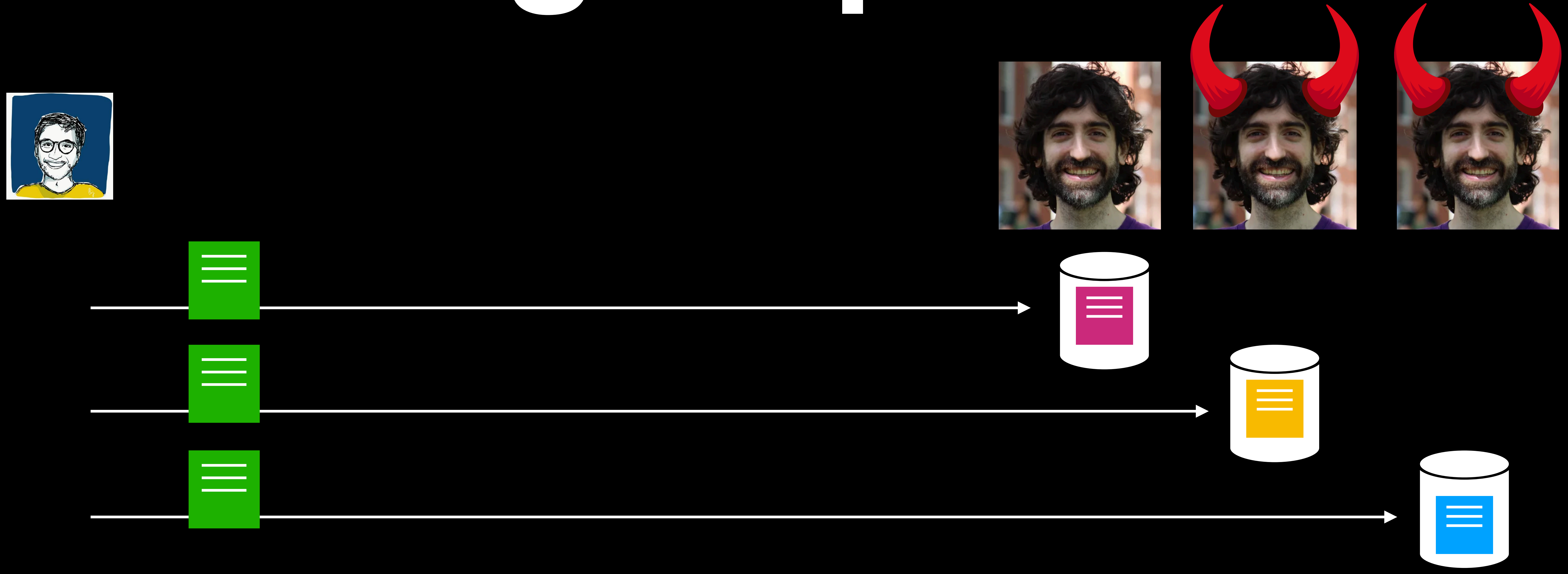
Proof of Retrievability



Proof of Retrievability



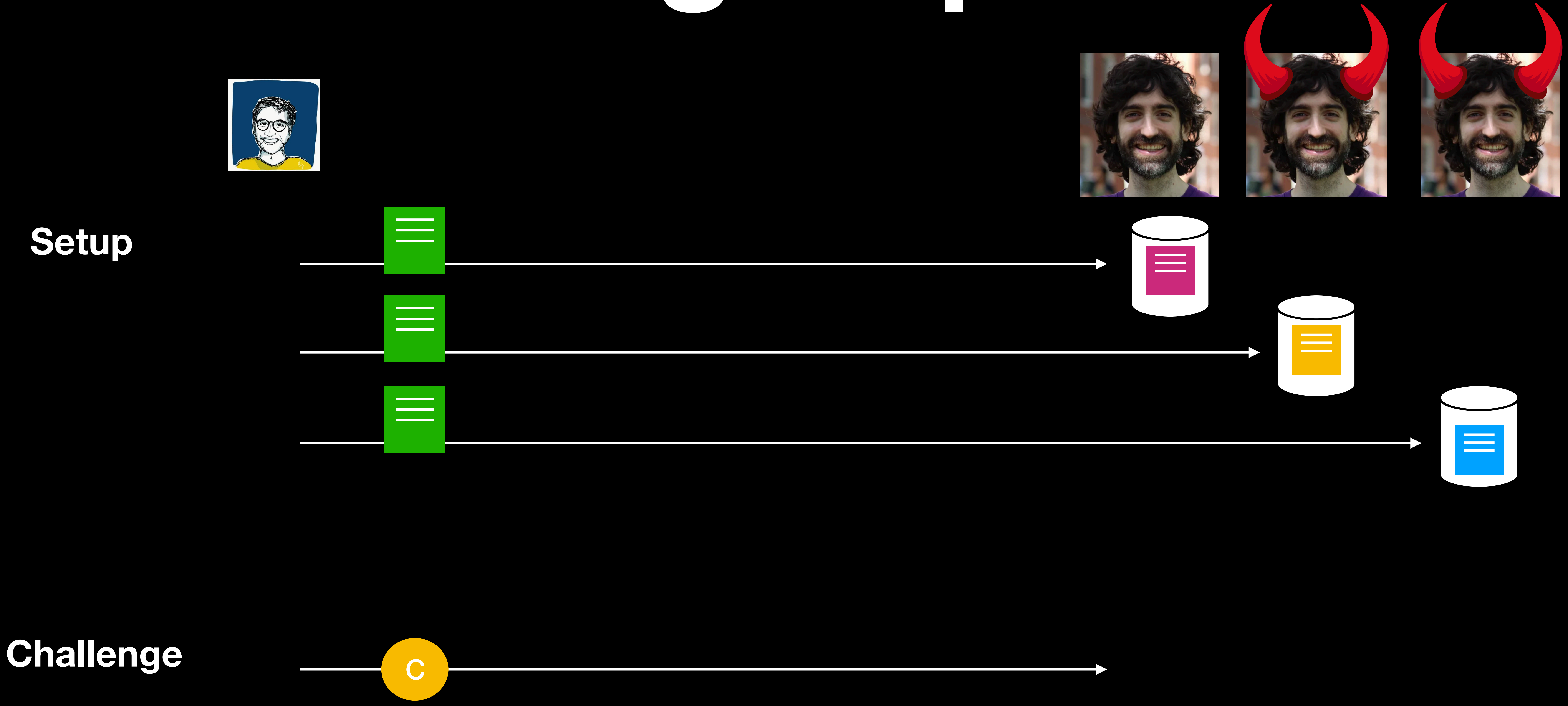
Adding Replicas



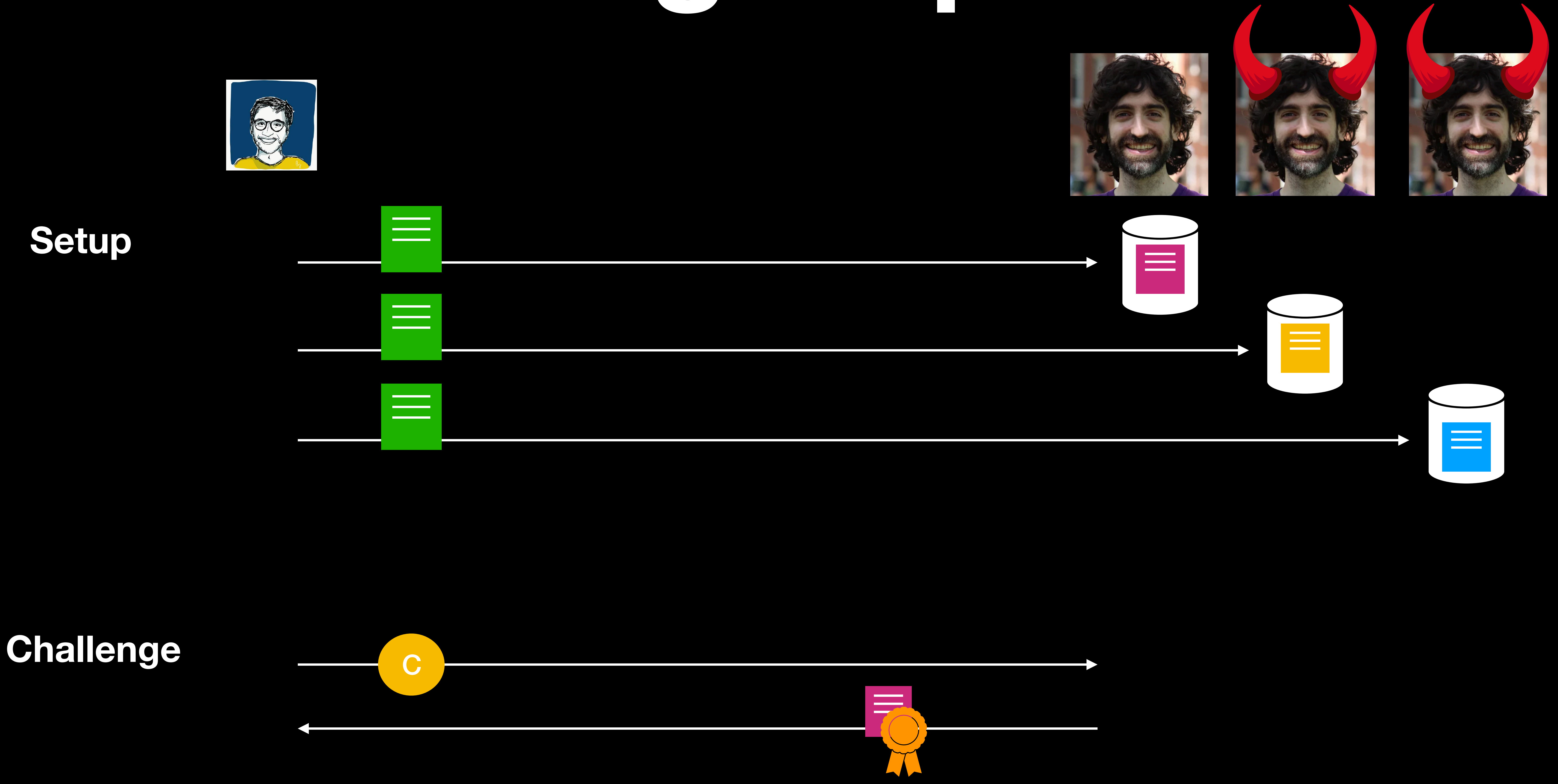
Setup

Challenge

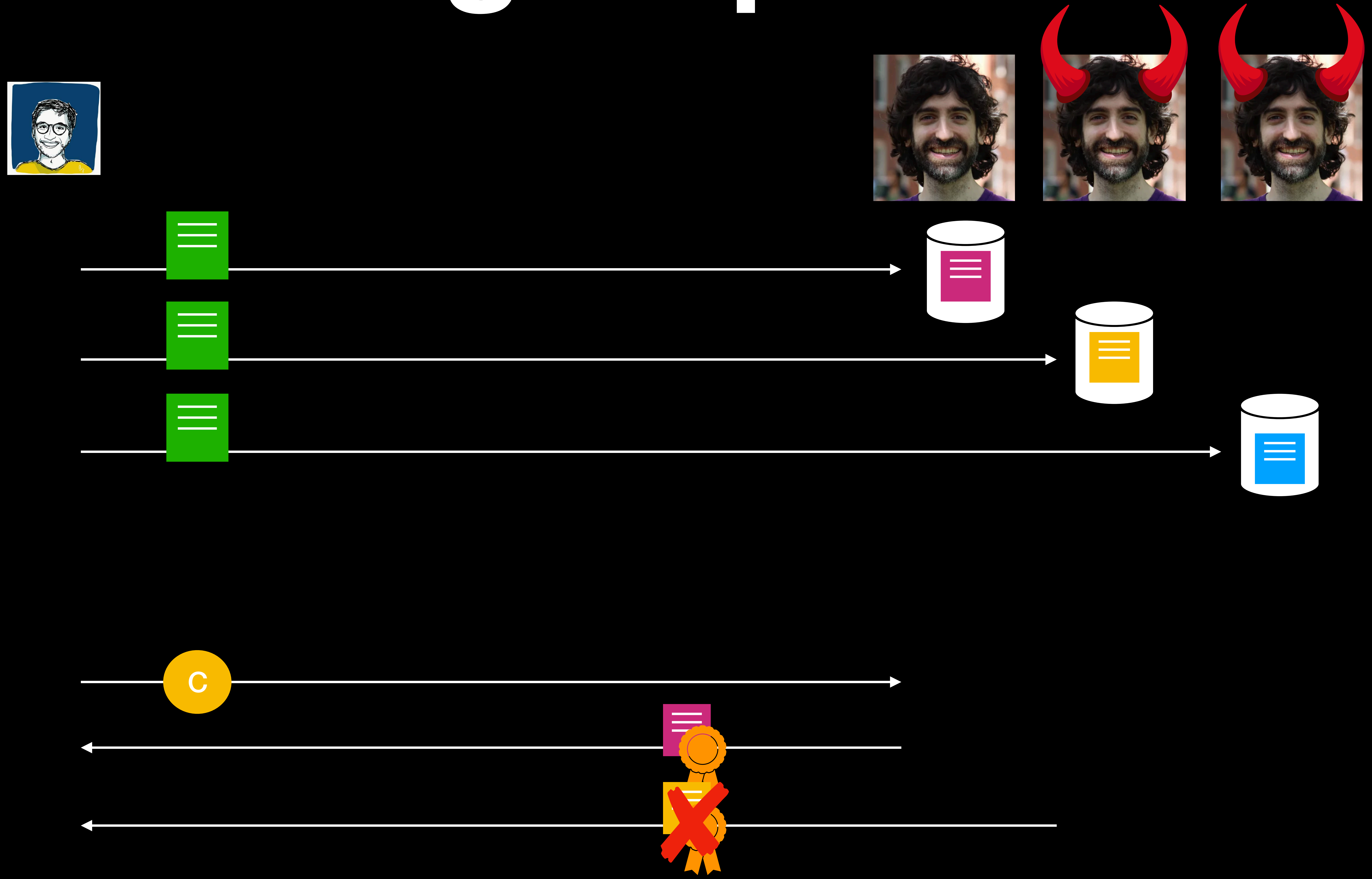
Adding Replicas



Adding Replicas



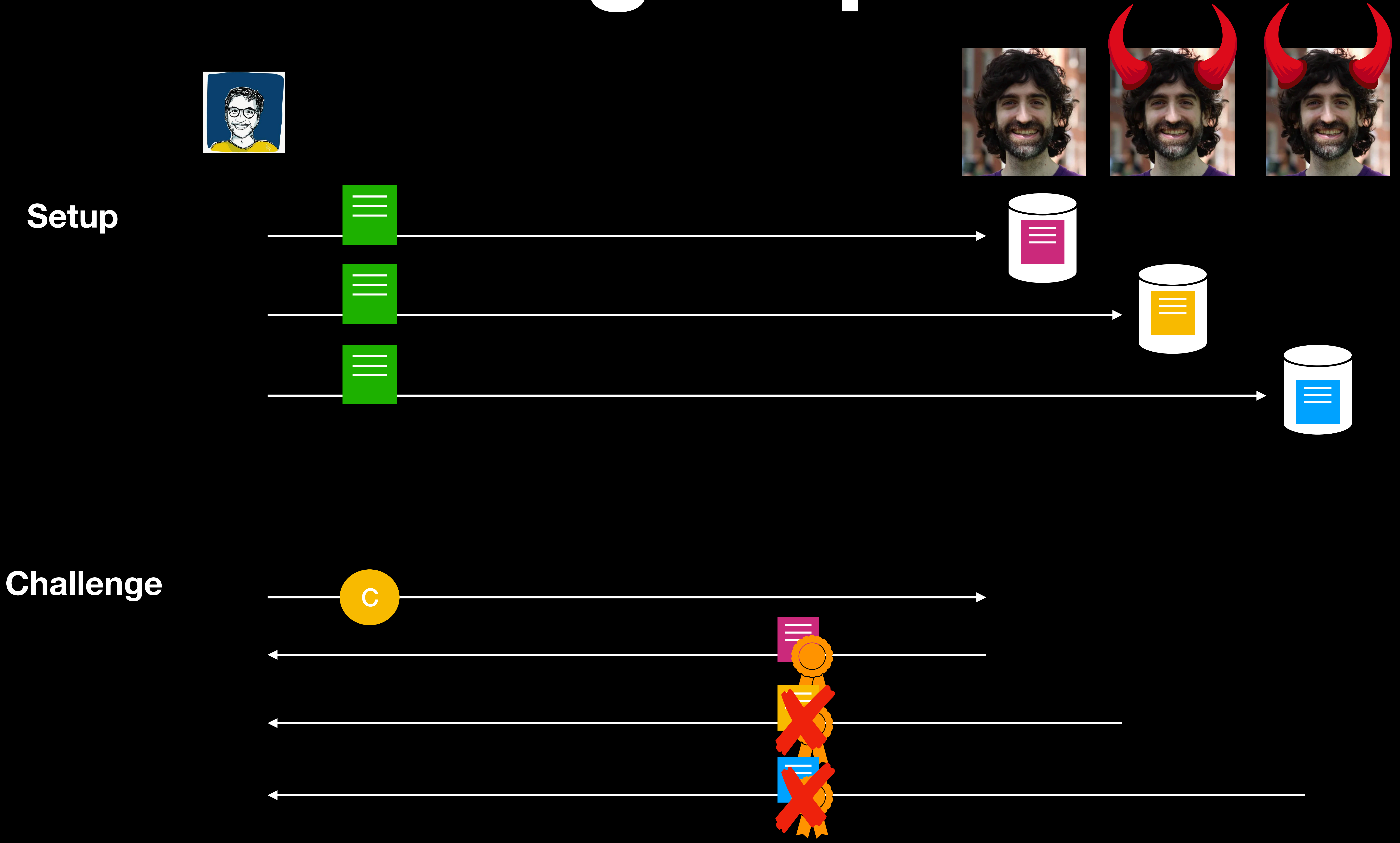
Adding Replicas



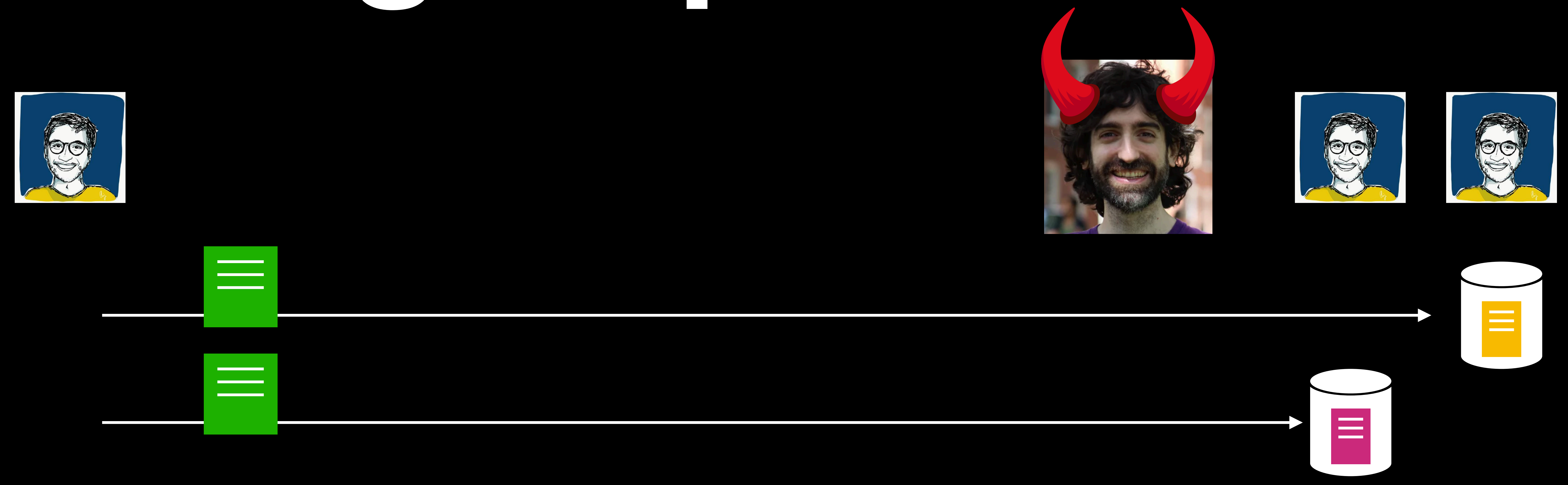
Setup

Challenge

Adding Replicas

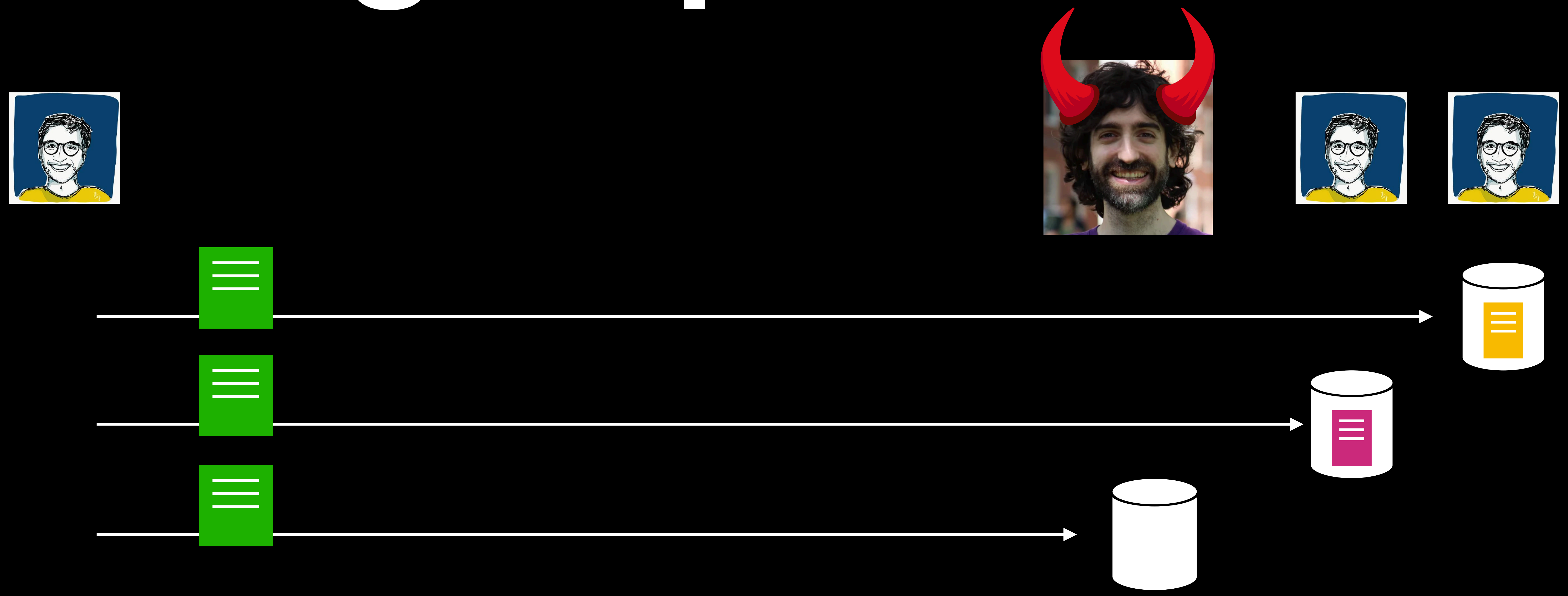


Making Replicas slow



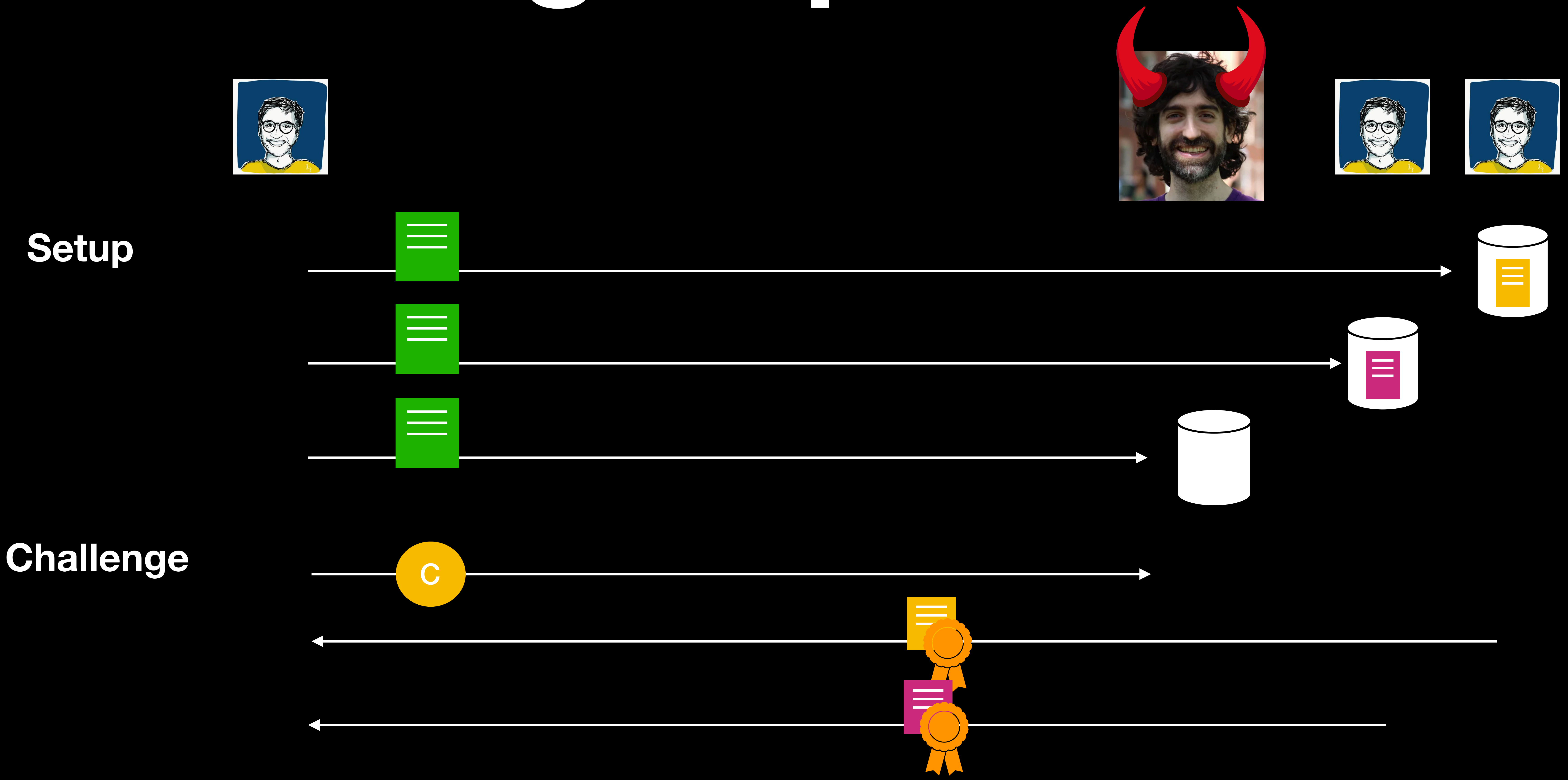
Setup

Making Replicas slow

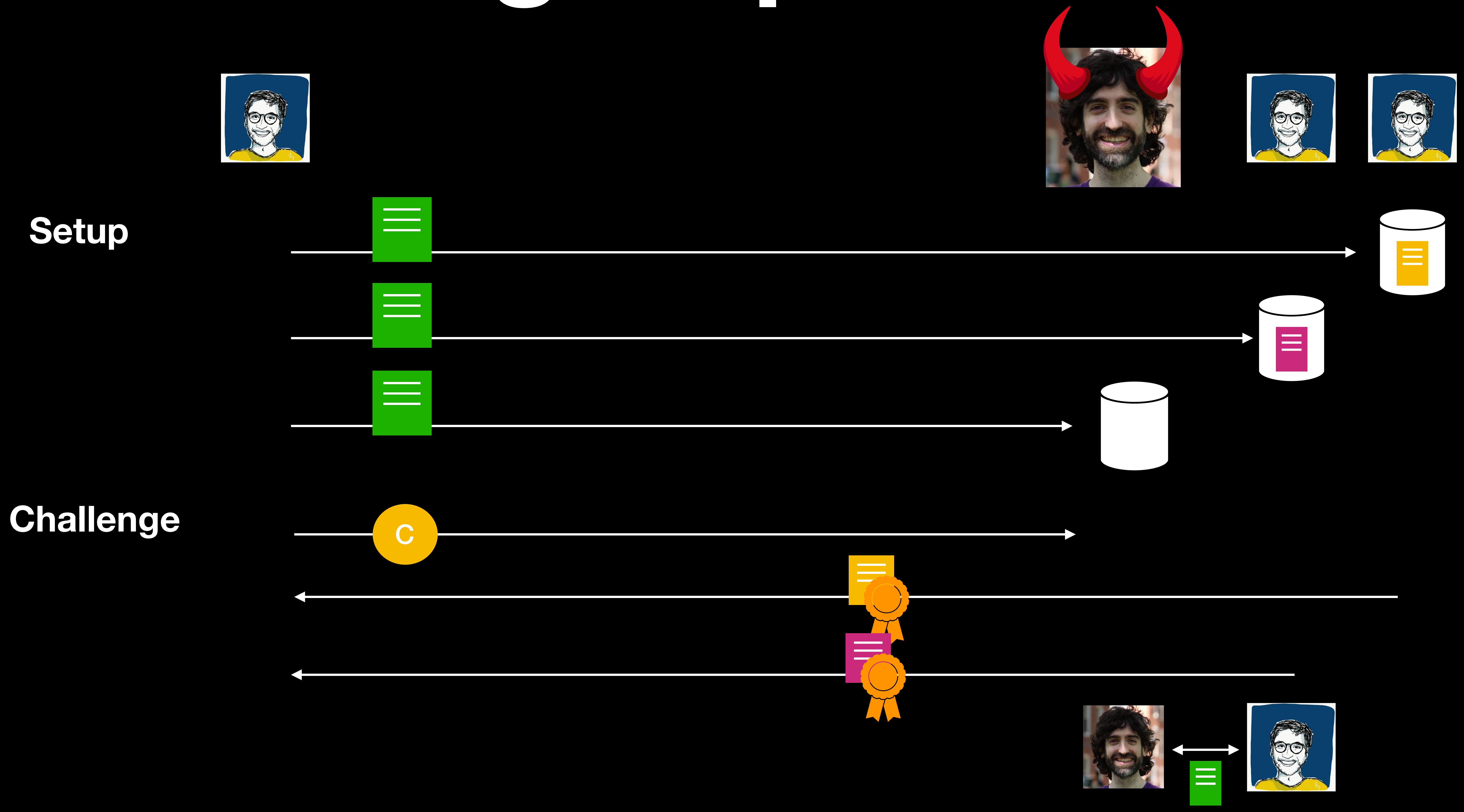


Setup

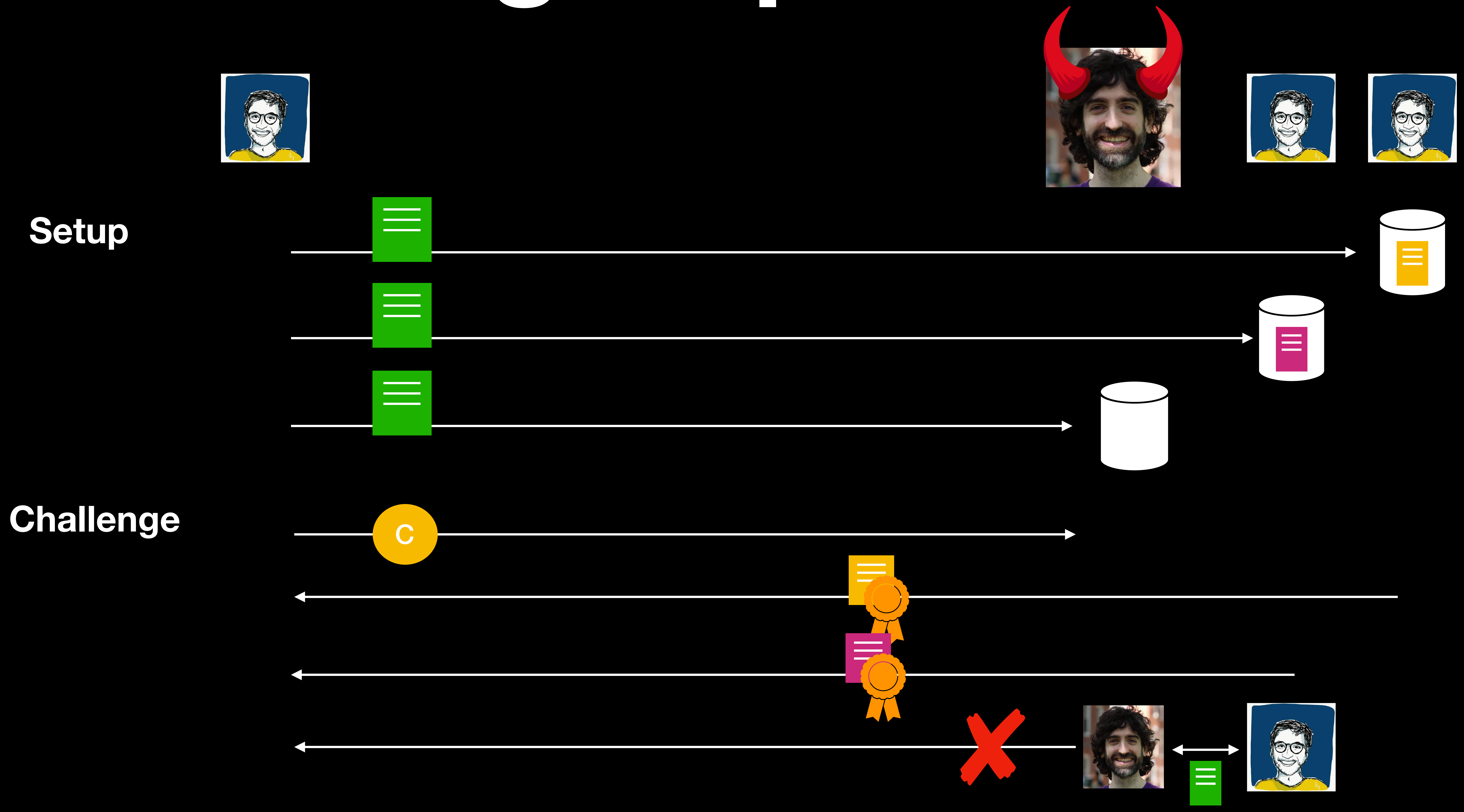
Making Replicas slow



Making Replicas slow



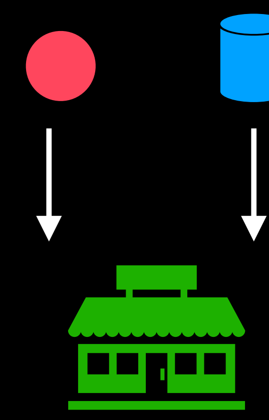
Making Replicas slow



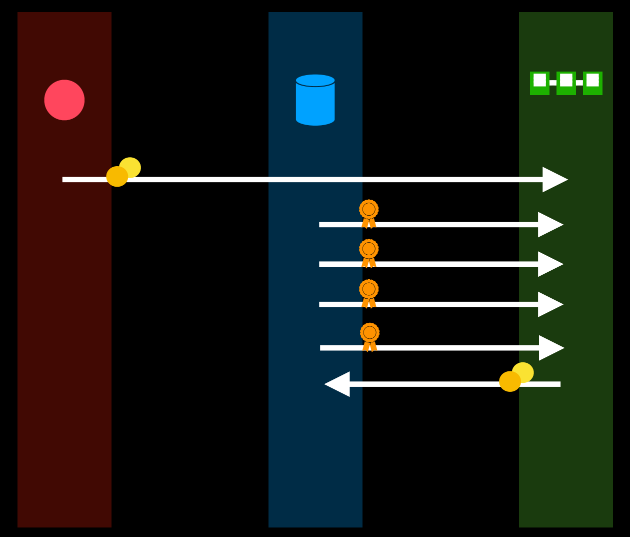
Filecoin Markets

Exchange

Order matching

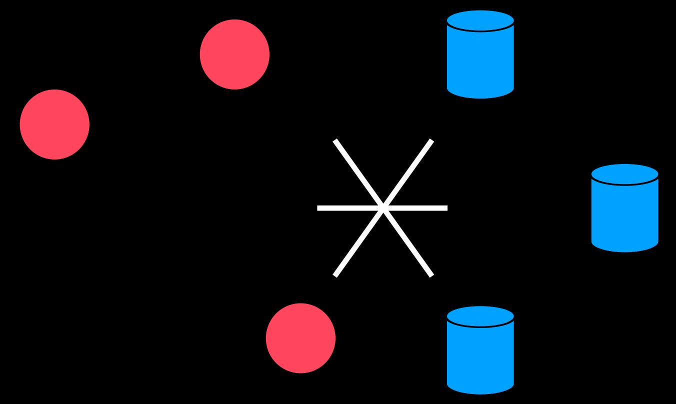


Settlement

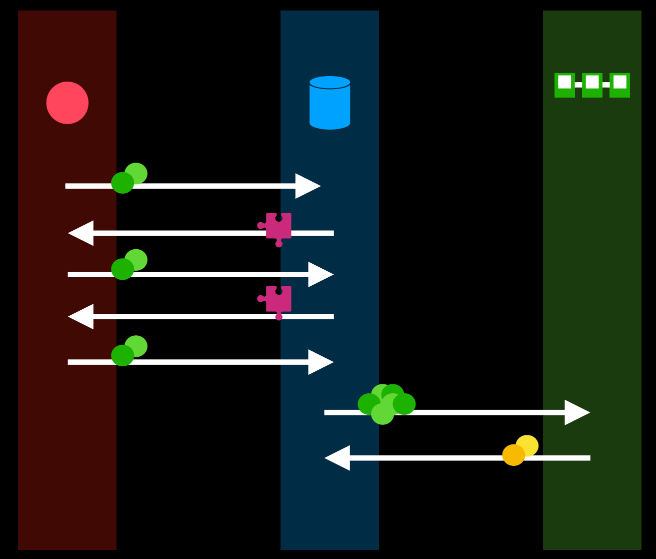


OTC

Order matching



Settlement

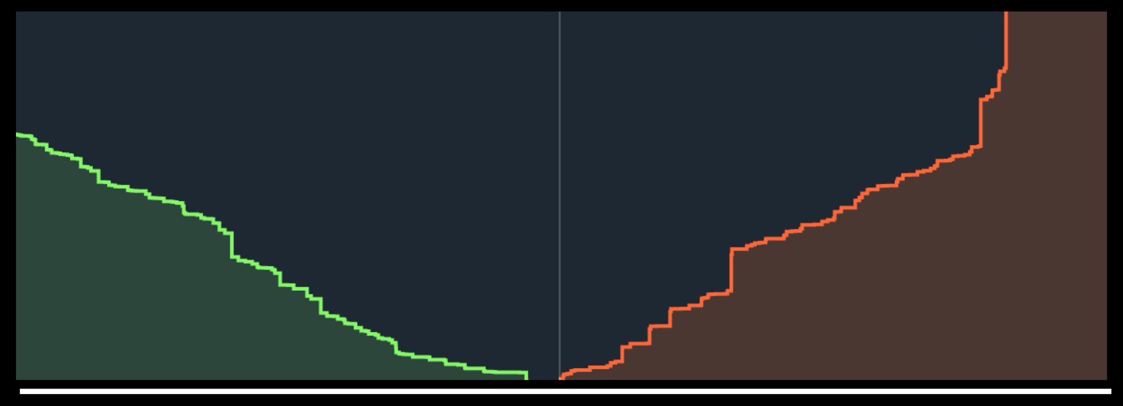


Order Matching

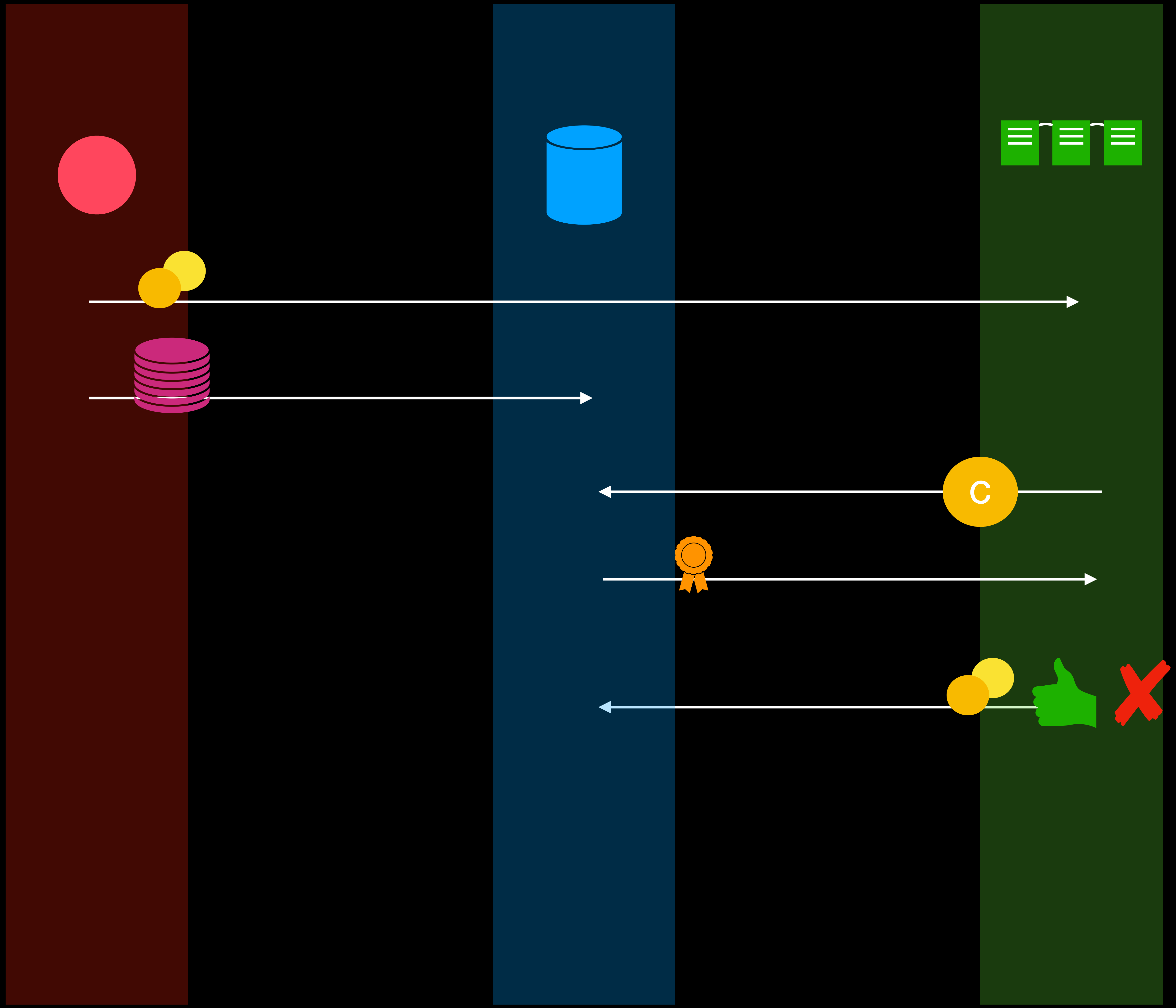
Storage/ Retrieval orders

Store a file
for 1 week
at 50c GB/h

Offer storage
for 1 week
at 50c GB/h

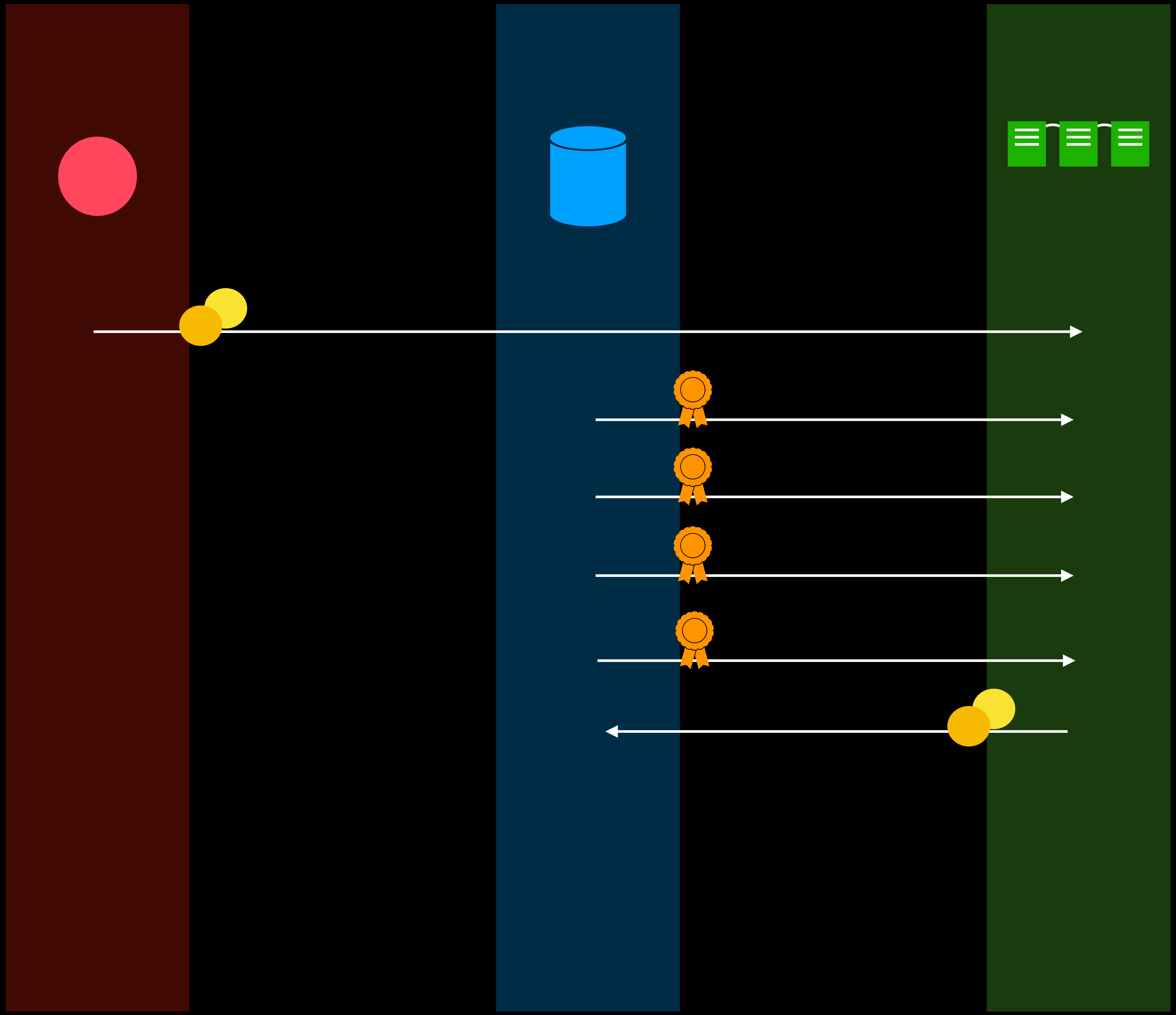


Paying for storage

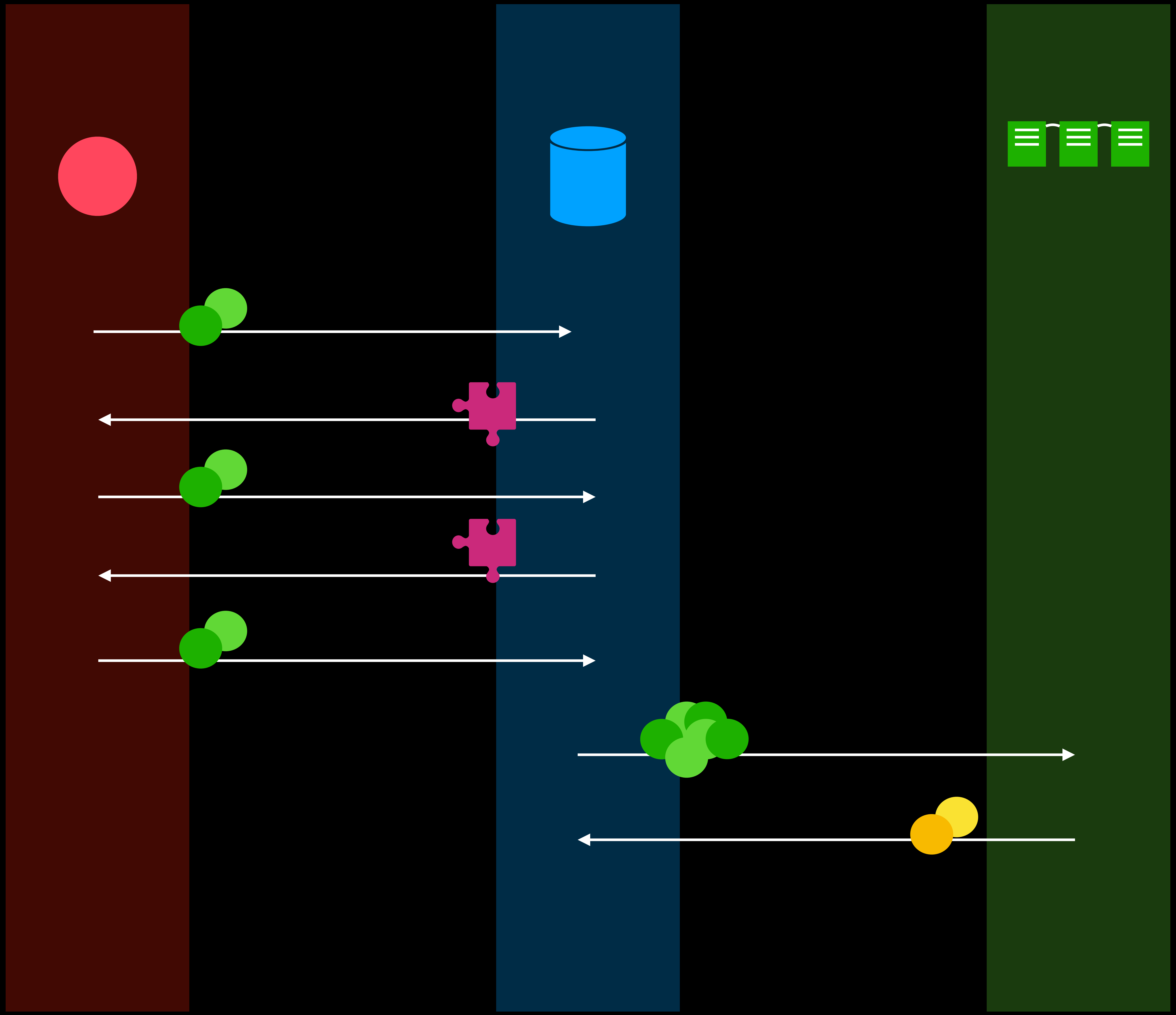


Verify

Storage Settlements



Retrieval Settlements



Storage-based Proof of Work

Open Questions

Are there ways to do efficient proofs of replication?

Are there ways to overcome front-running attacks?

Are there ways to avoid miners posting proofs on chain?

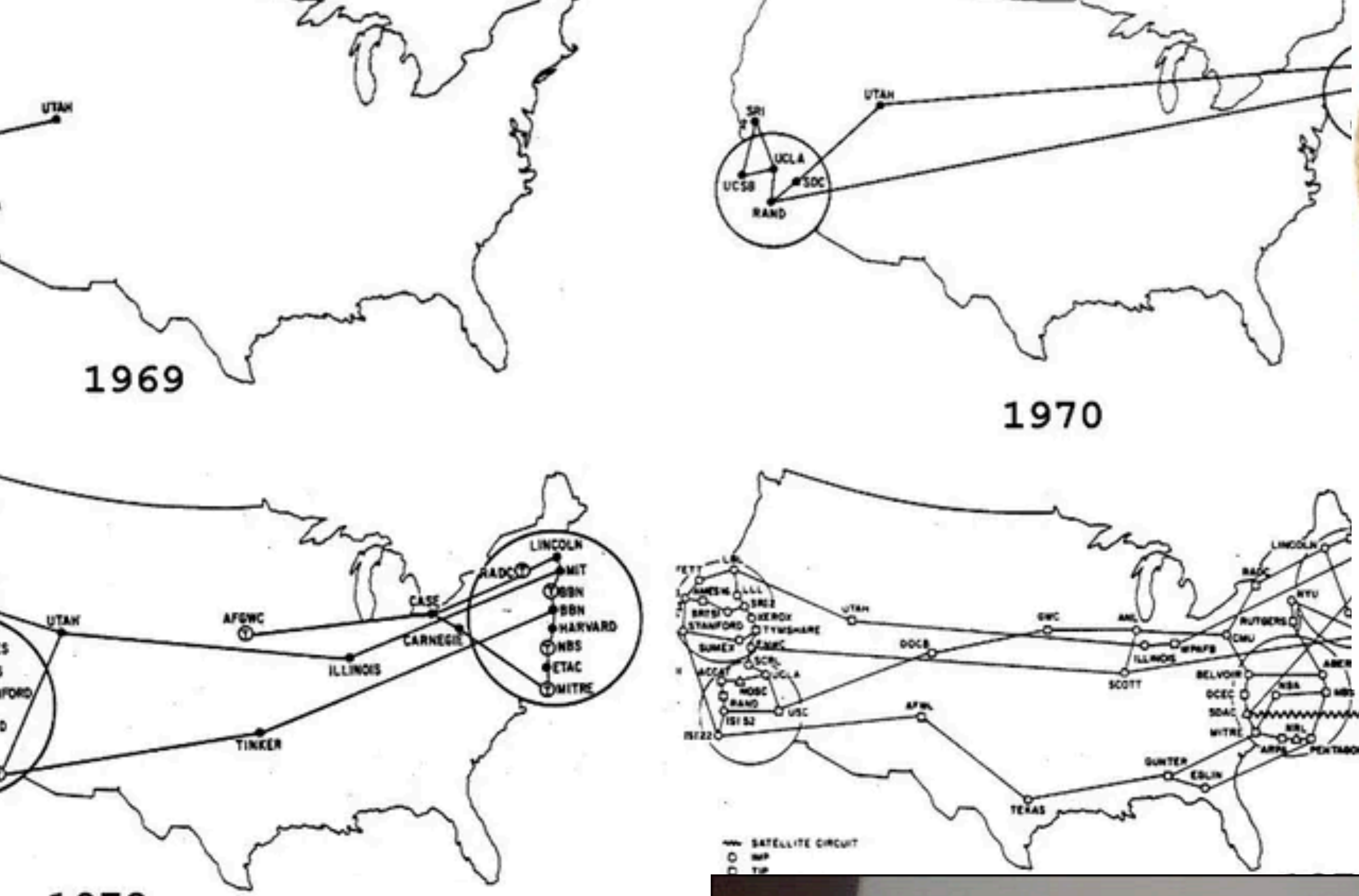
Can build a storage-based consensus?

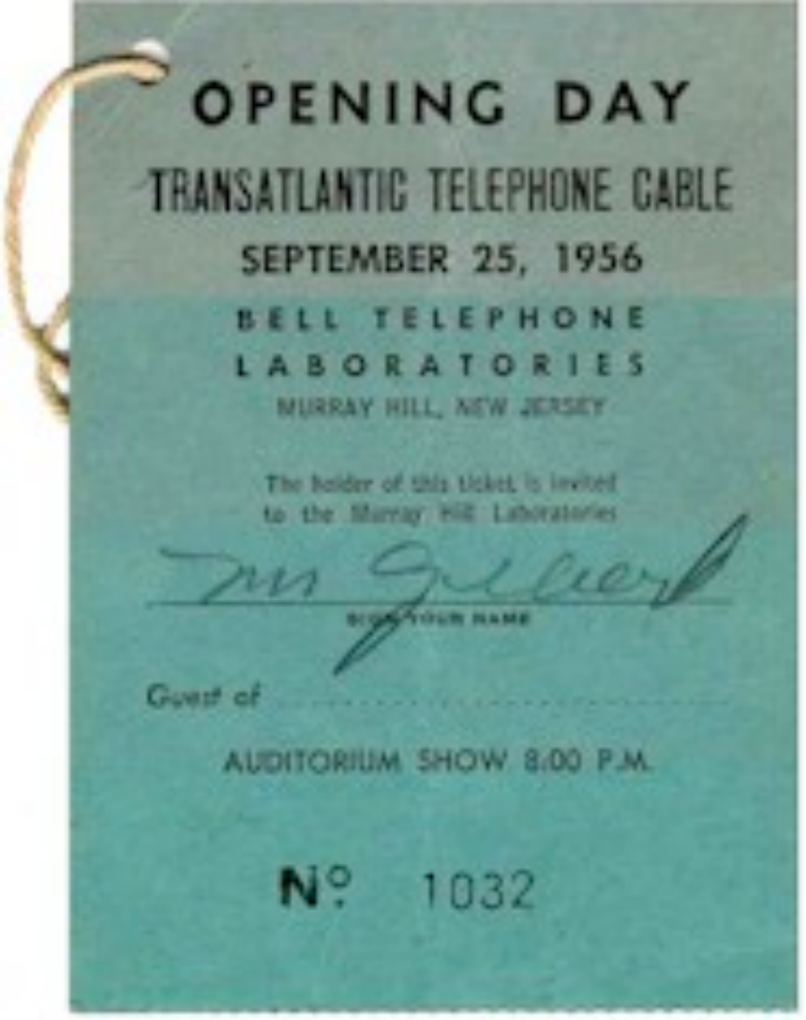
What are other incentives beyond economic reward?

Part 4

Foundational Infrastructure

Bell Labs Holmdel site





OPENING DAY

TRANSATLANTIC TELEPHONE CABLE

SEPTEMBER 25, 1956

BELL TELEPHONE LABORATORIES

MURRAY HILL, NEW JERSEY

The holder of this ticket is invited to the Murray Hill Laboratories

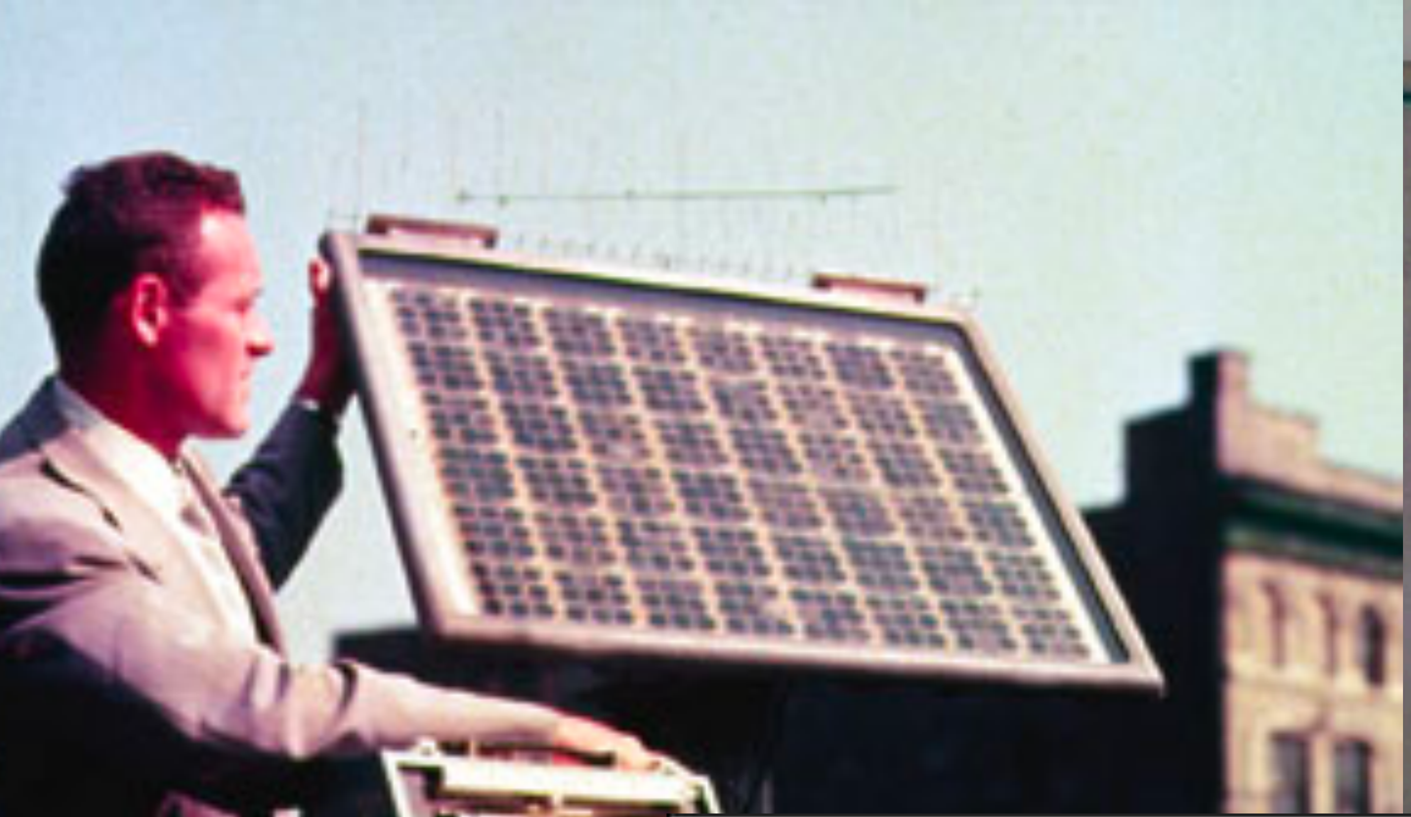
Mr Gilbert

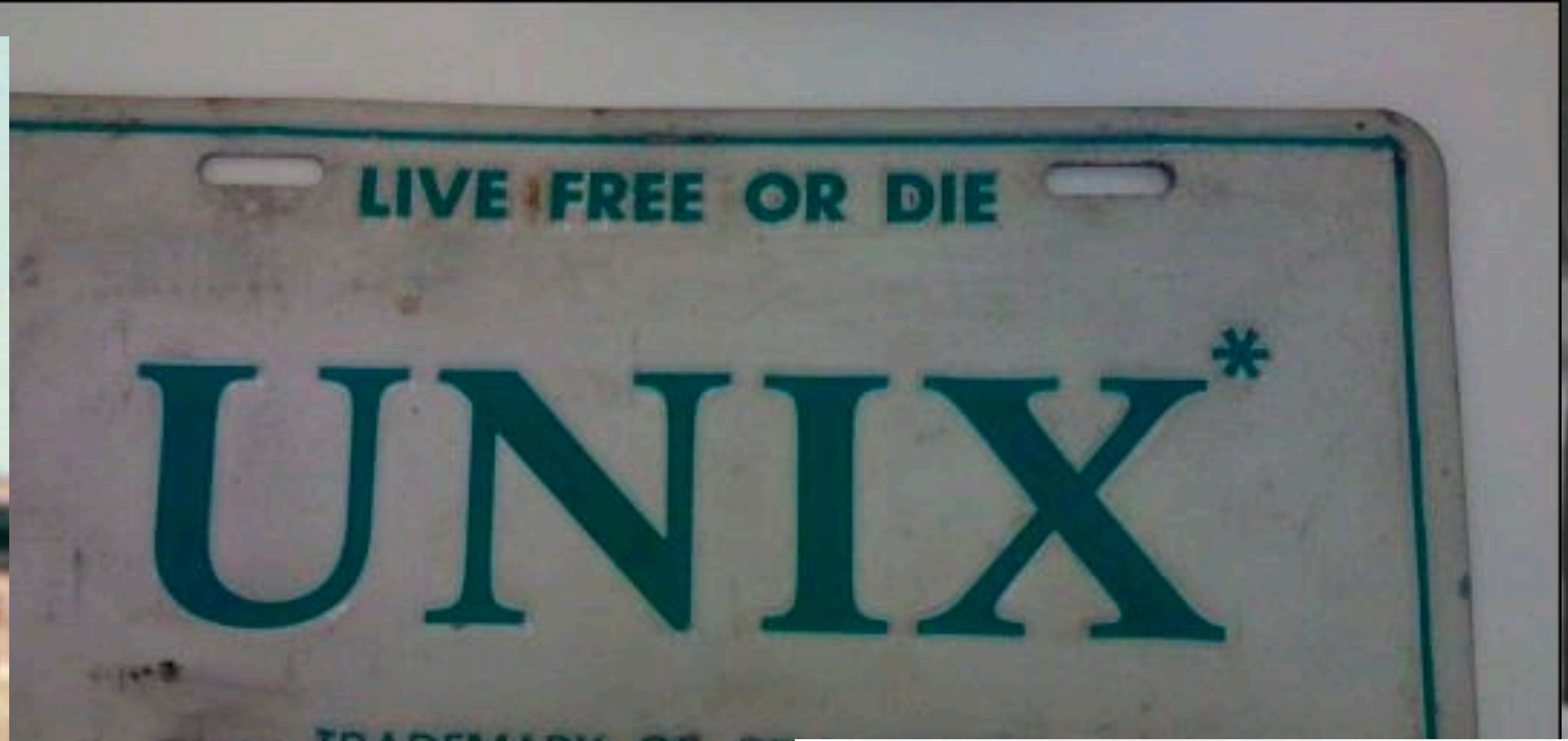
SIGN YOUR NAME

Guest of

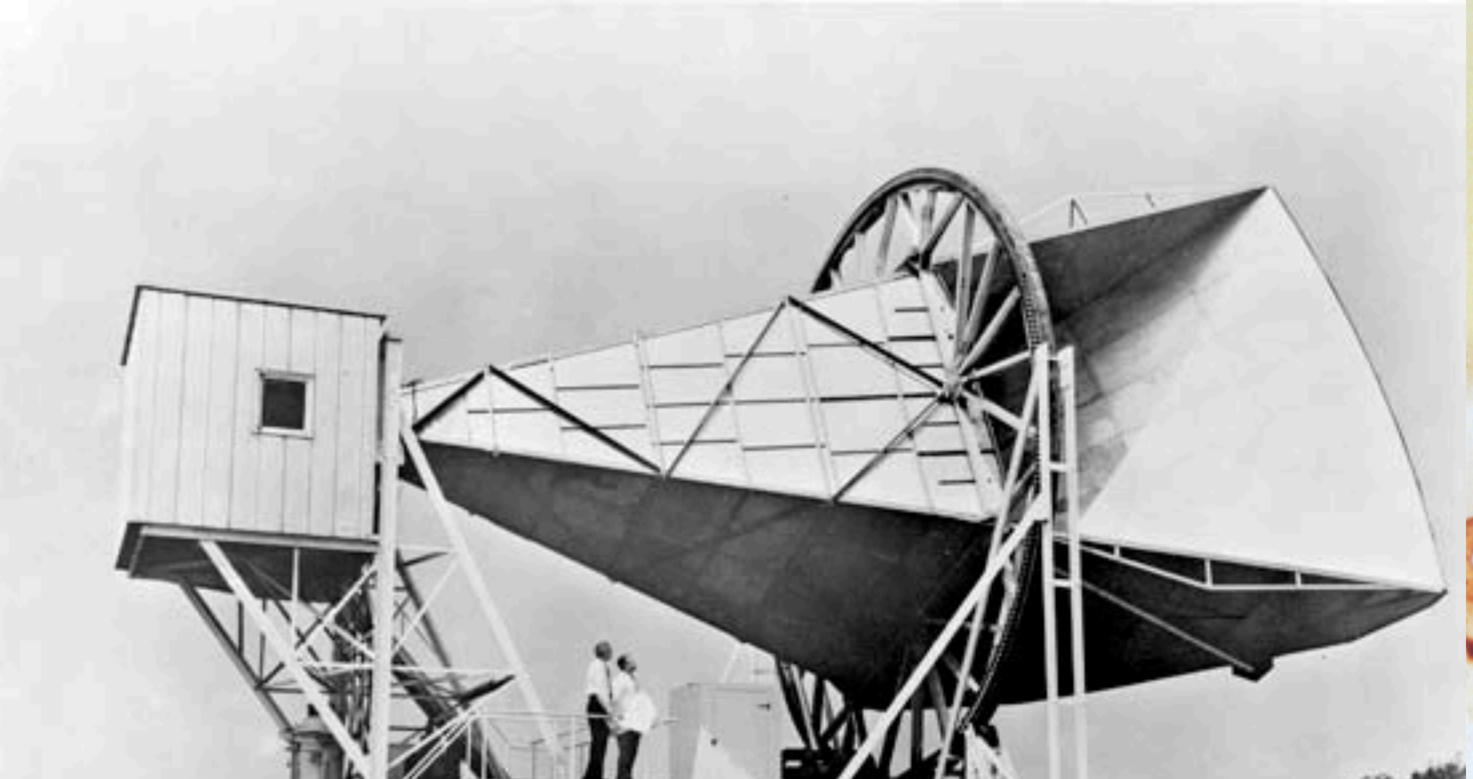
AUDITORIUM SHOW 8:00 P.M.

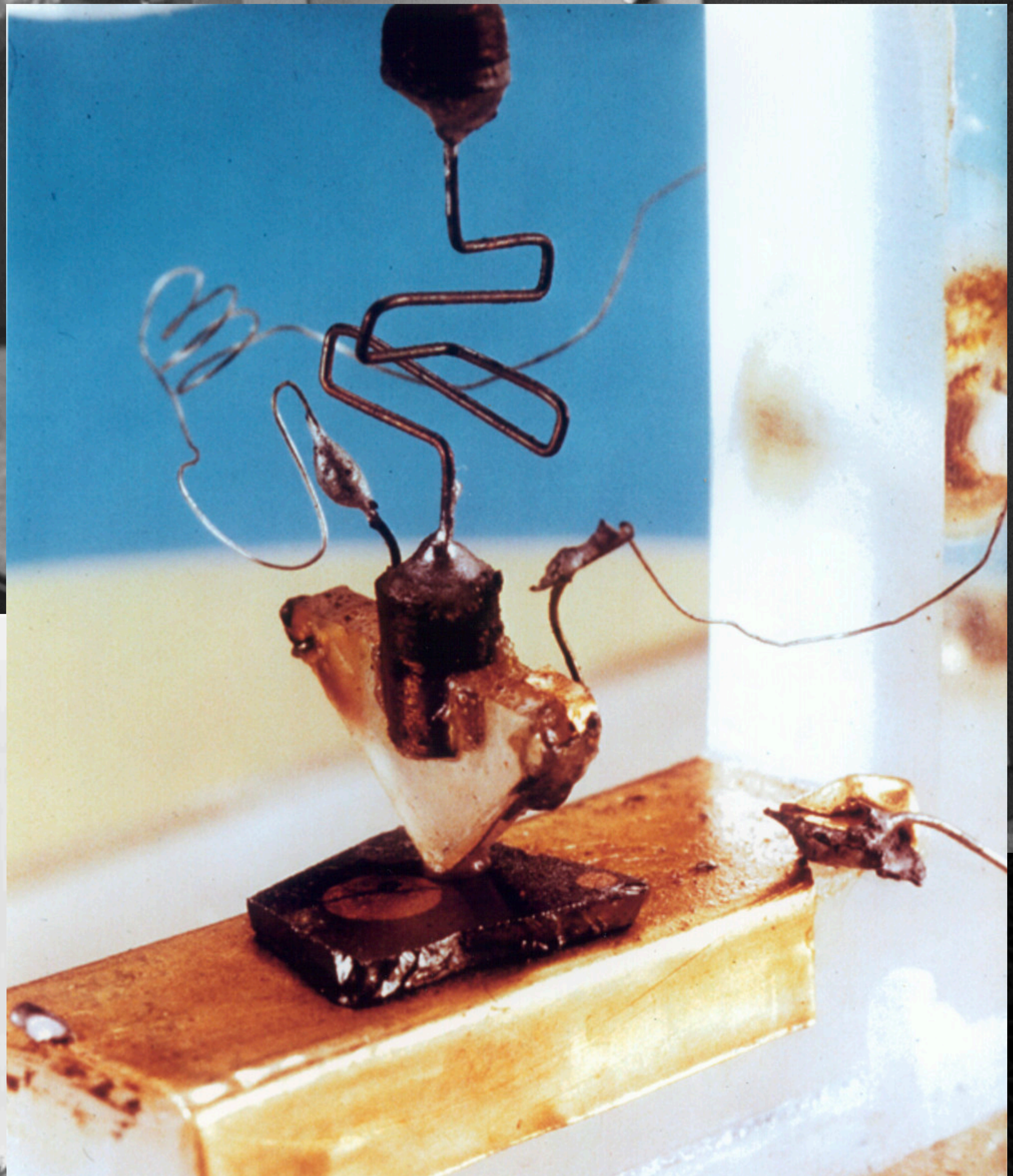
Nº 1032





THE C PROGRAMMING LANGUAGE





Open Source

Open Source

THE LINUX FOUNDATION

Open Source

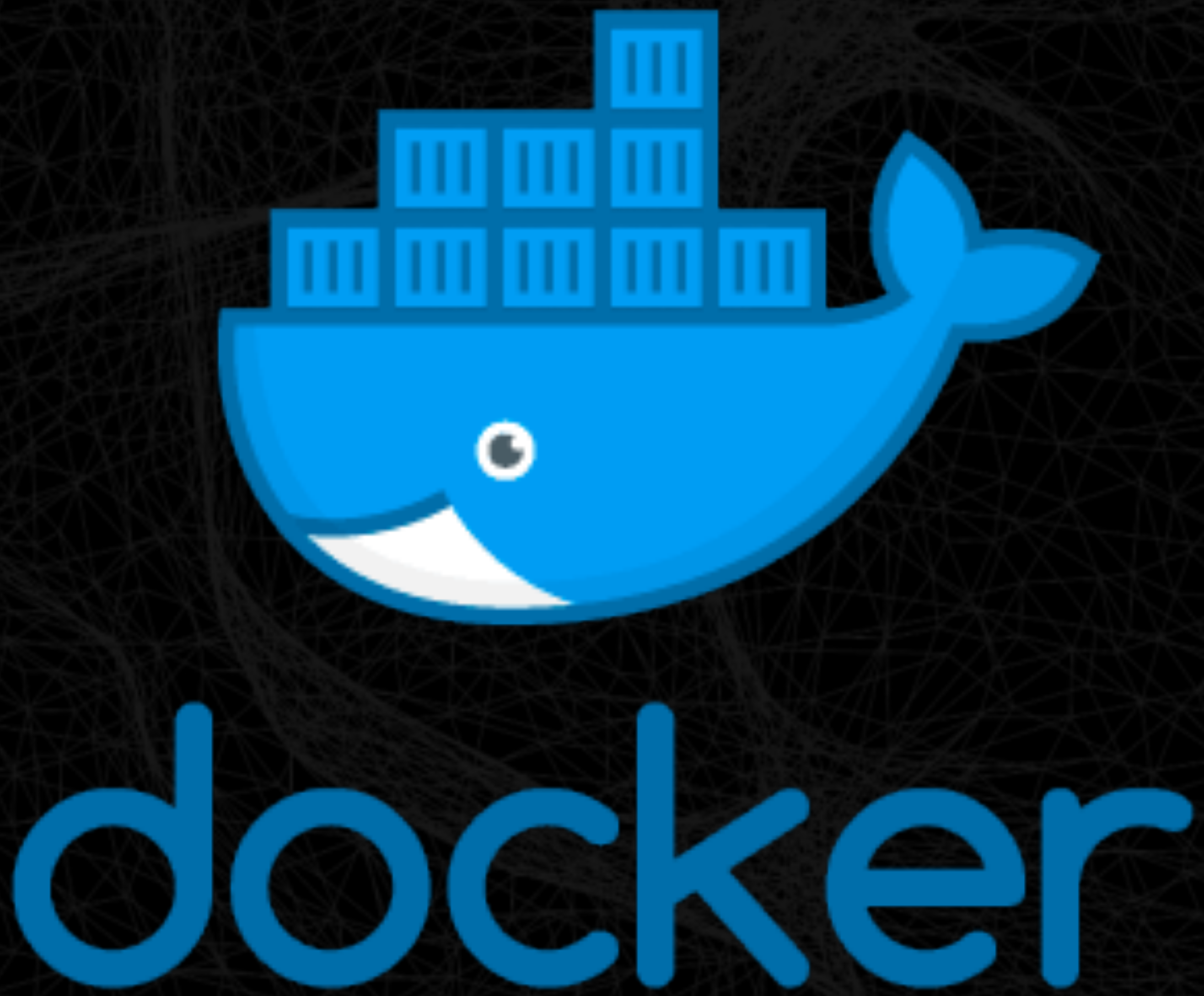
THE LINUX FOUNDATION

TM

Open Source

docker

Open Source



Open Source

Open Source

Open Source

Open Source

THE LINUX FOUNDATION
node JS®
open source hardware TM
JS
THE APACHE® SOFTWARE FOUNDATION
docker

THE LINUX FOUNDATION
node JS®
open source hardware TM
JS
firefox
THE APACHE® SOFTWARE FOUNDATION
docker

Open Source

Open Source

THE LINUX FOUNDATION
node JS®
open source hardware TM
JS
THE APACHE® SOFTWARE FOUNDATION
firefox®
docker

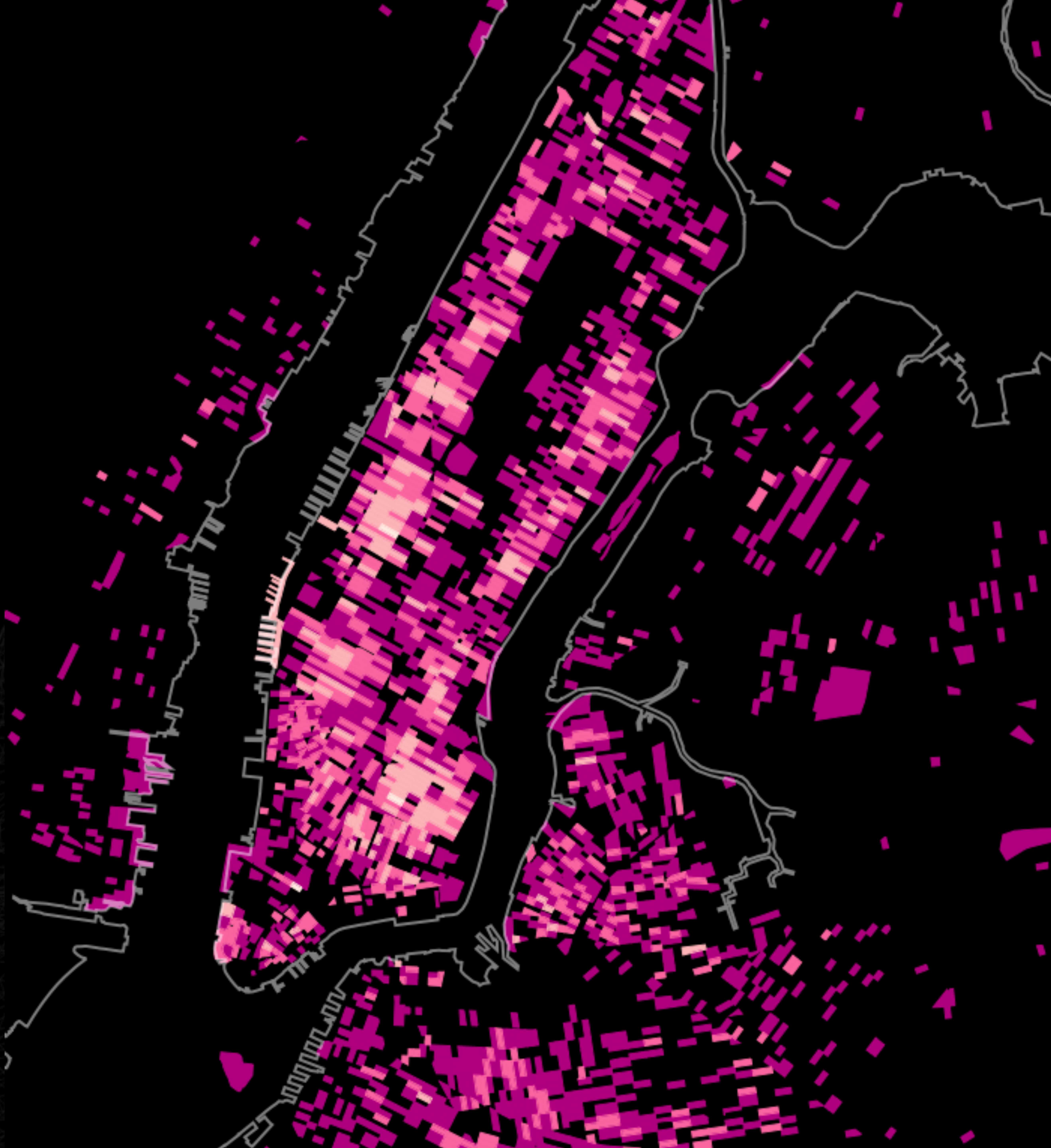
THE LINUX FOUNDATION
node JS®
en sourc
ardware
TM
THE Open S rc
APACHE®
SOFTWARE FOUNDATION
JS
refox
gi
docker

THE
LINUX
FOUNDATION
node
JS
en sourc
ardware
TM
JS
THE Open S rc
APACHE
SOFTWARE FOUNDATION
refox
gi
docker

THE LINUX FOUNDATION
node JS®
IPFS
JS
THE Open S rc
APACHE®
SOFTWARE FOUNDATION
firefox
git
docker

Sharing Economy

airbnb



Crypto Network & Tokens

USB 2.0
DVB-T+DAB+FM

Hash Rate

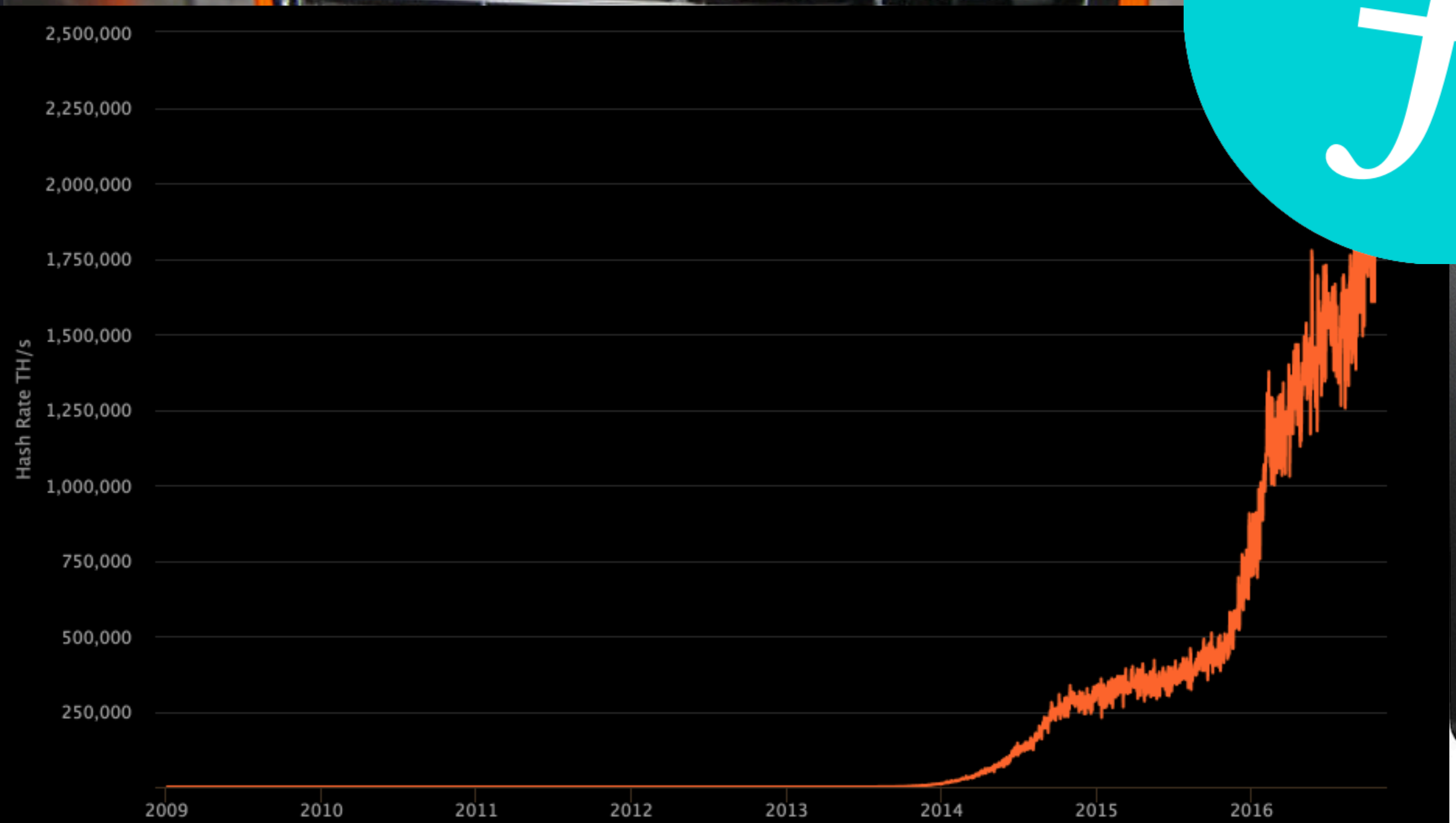
source: blockchain.info

TOP500®
SUPERCOMPUTER SITES
Hash Rate TH/s
15,000,000
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17

Filecoin

bitcoin + amazon web services™ | S3

IPFS


2,500,000
2,250,000
2,000,000
1,750,000
1,500,000
1,250,000
1,000,000
750,000
500,000
250,000
Hash Rate TH/s
2009
2010
2011
2012
2013
2014
2015
2016

TS-879Pro
169.254.100.100
QNAP
ENTER
SELECT
POWER
COPY

Maxtor

Canada
Bermuda
México
Cuba
Haiti
Venezuela
Guyana
Colombia
Ecuador
Perú
Brasil
Bolivia
Paraguay
Algérie
الجزائر
ليبيا
Niger
Tchad
Nigeria
South Sudan
Liberia
São Tomé e Príncipe
Saint Helena Ascension and Tristan da Cunha
Madagascar
Россия
Казахстан
Тоҷикистон
Pakistan
British Indian Ocean Territory
Indonesia
Belau
Guam
Federated States of Micronesia
Marshall Islands
Nauru
Solomon Islands
Tuvalu
Australia
Norfolk Island
Kiribati
Tokelau
American Samoa
Tonga
Pitcairn Islands

Filecoin

store to
earn ⨍

exchange
for ₿ 💵

spend ⨍
to store

USER
STORAGE SERVER
STORAGE SERVER
WEST
CLINTON
HILL
USS Intrepid
W 57th St
W 54th St
E 66th St
Plaza Hotel
9th Ave
Museum of
Modern Art
Rockefelle
Universit
HELL'S
KITCHEN
DIAMOND
W 42nd St
Park Ave
Lexington Ave
2nd Ave
1st Ave
FDR Dr
12th Ave
W 36th St
W 34th St
W 31st St
E 46th St
Trump World
Tower
United Nations
KOREATOWN
MURRA
H
EA

Free Market for Data Storage

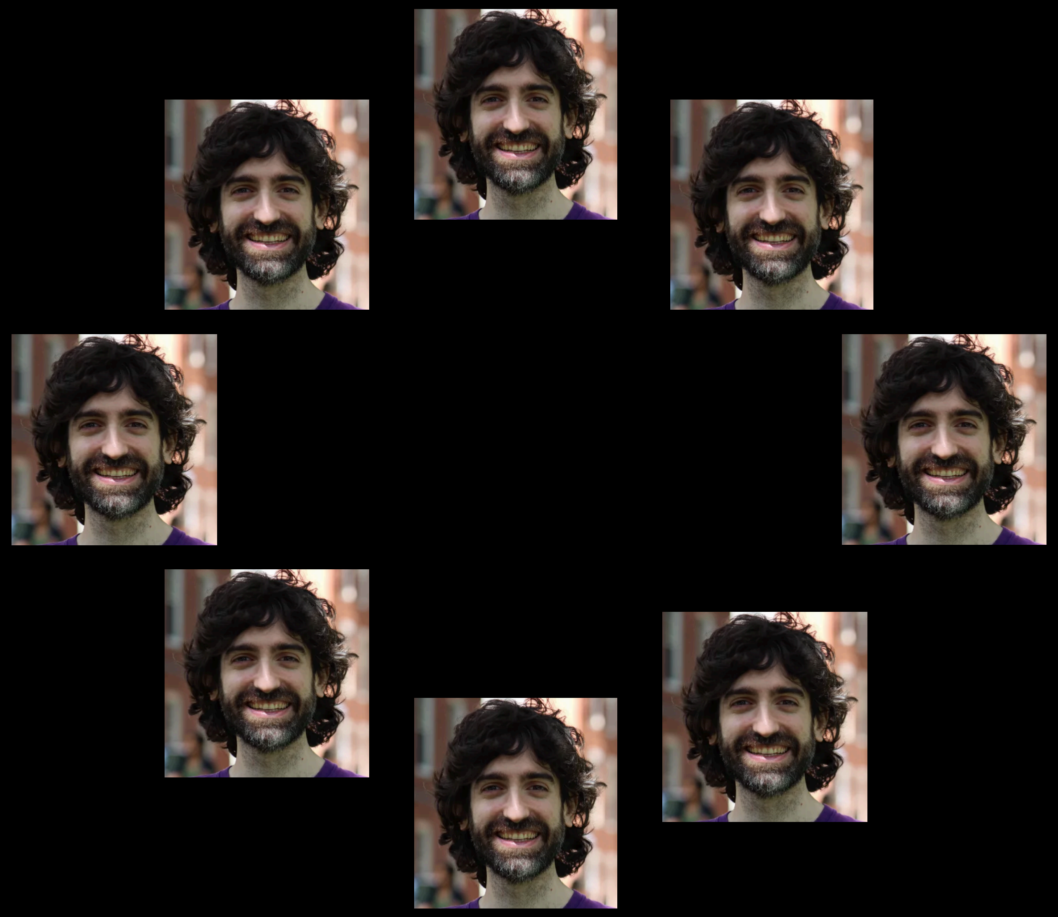
10k
8k
6k
4k
2k
0
⨎5.99
⨎6.00
⨎6.01
⨎6.02
⨎6.03
⨎5.2
⨎5.4
⨎5.6
⨎5.8
⨎6.2
⨎6.4
⨎6.6
⨎6.8

Governance?

github.com/nicola/
decentralized-research

Thank you
Samer

Thank you
Samer



Question?

What are other trust models? What is any-trust?

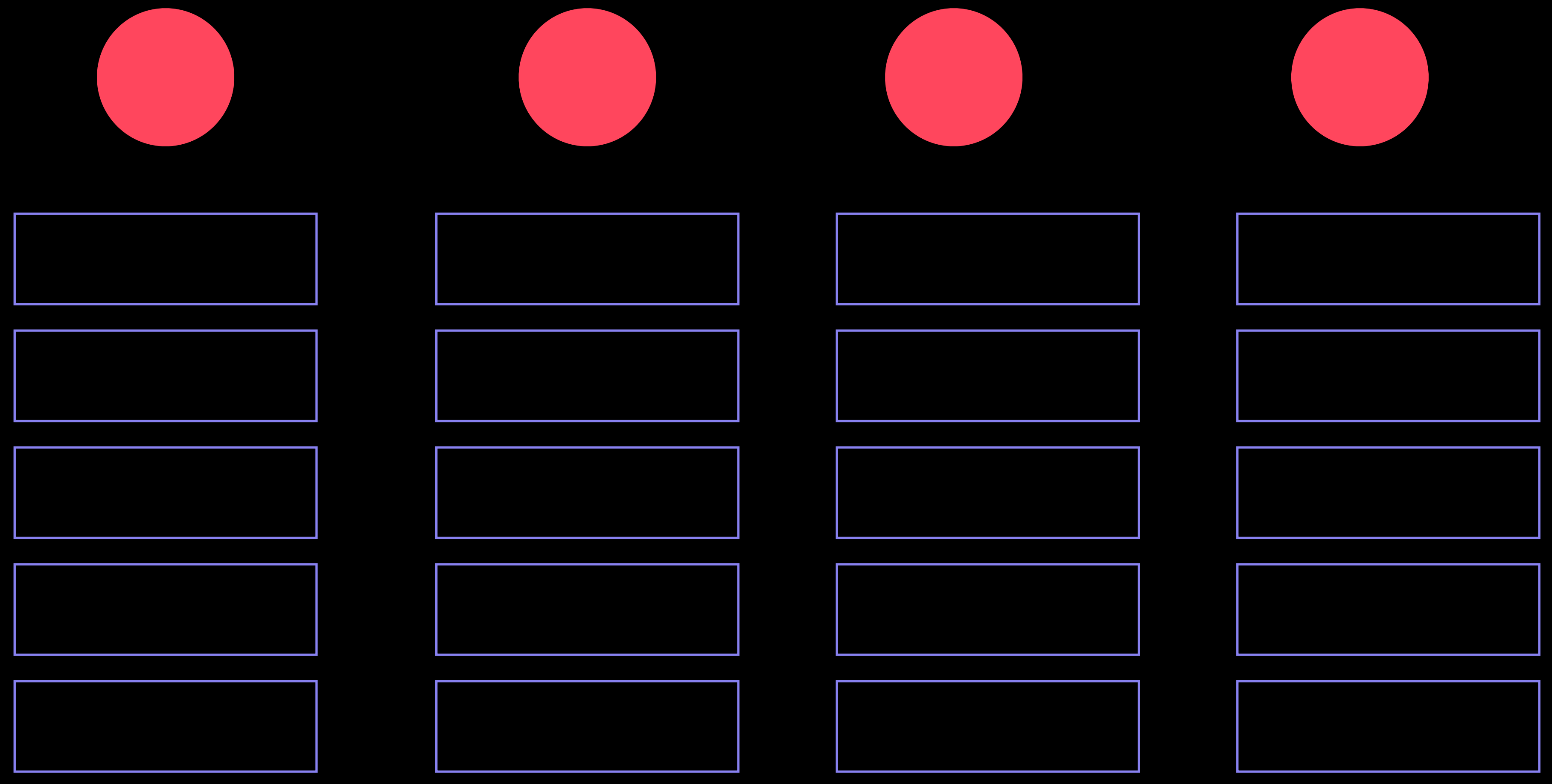
What are other types of Verifiable Markets?

Would this be enough for decentralizing the web?

Can DDoS attacks be possible on Filecoin?

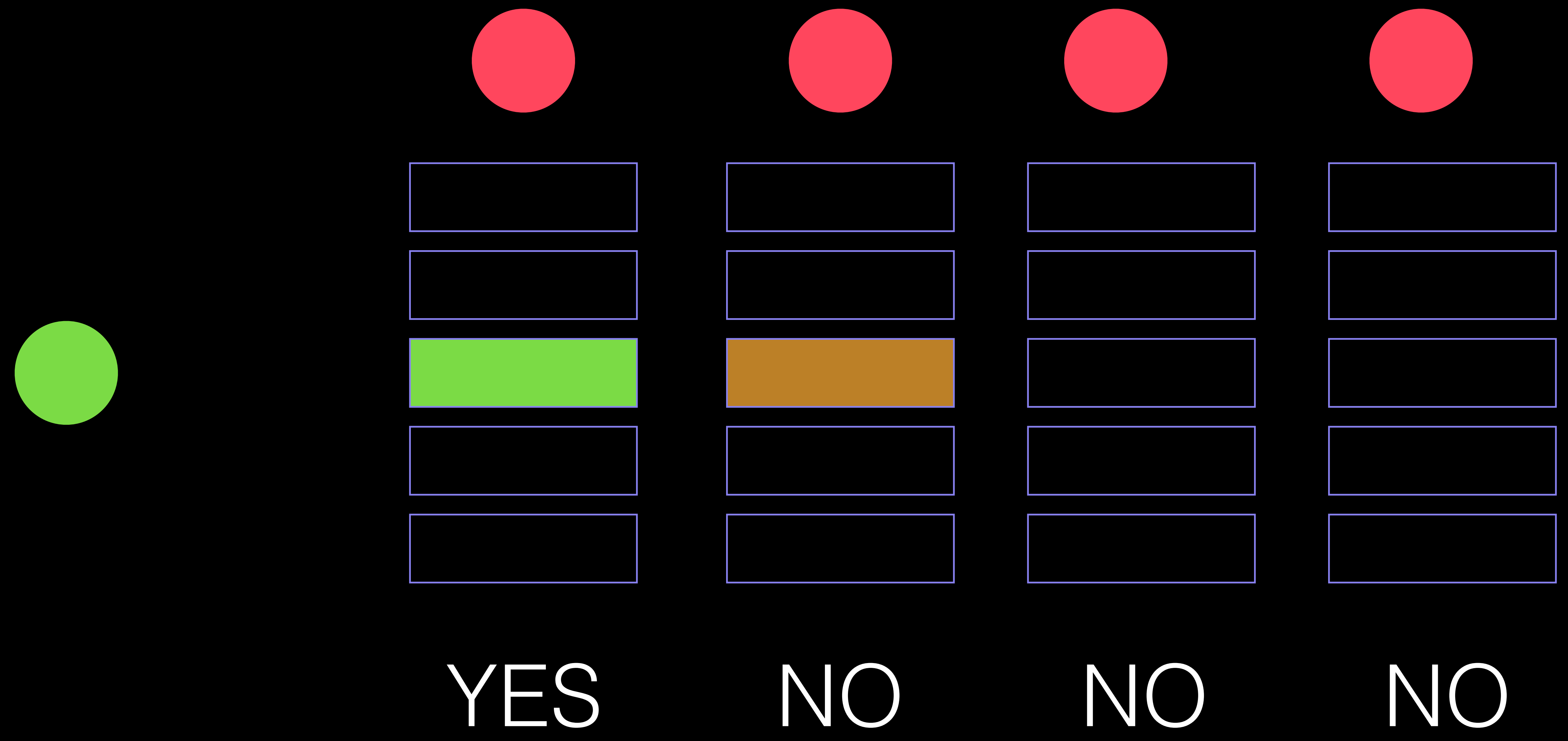
How do you know Samer?

Refereed Multi-Prover

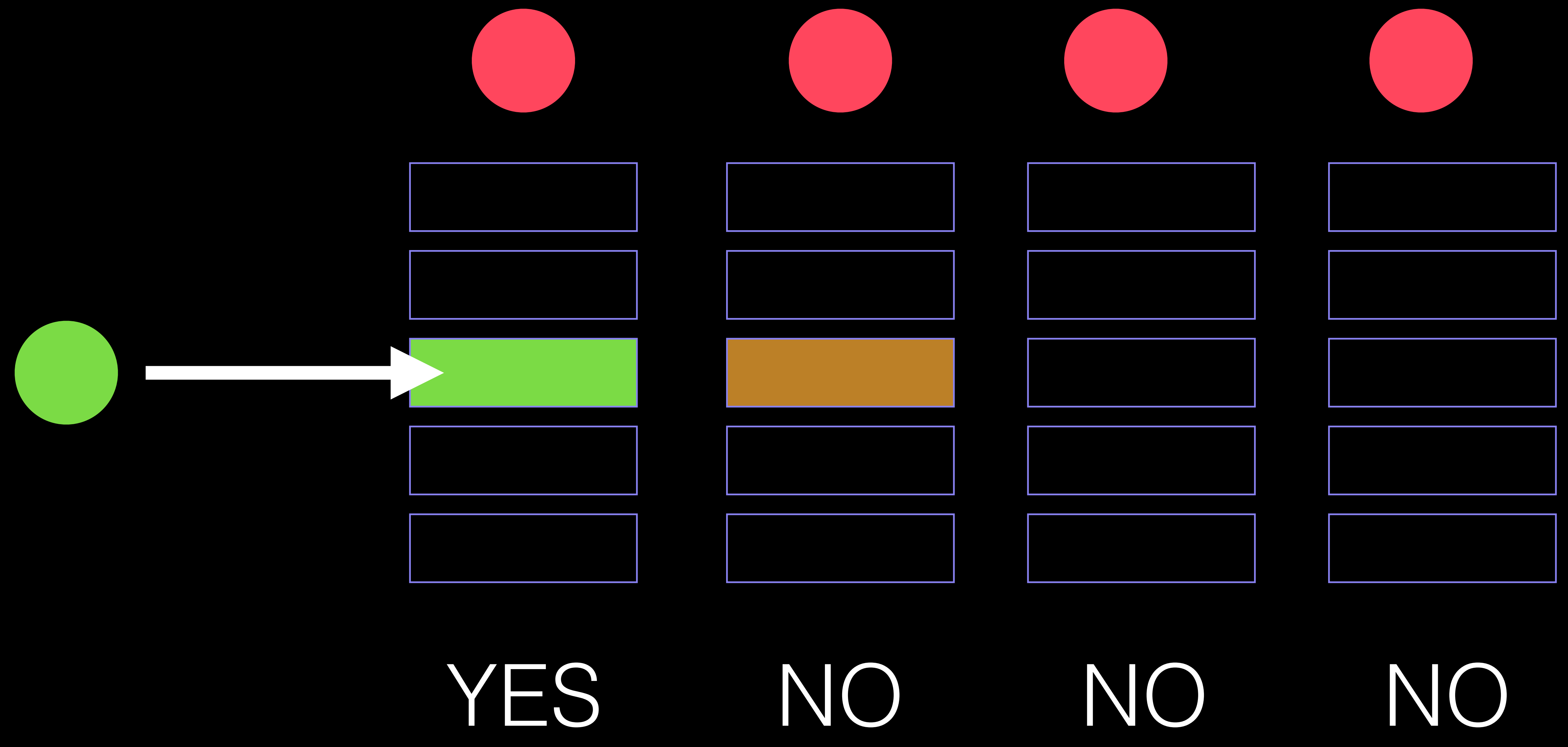


YES NO NO NO

Refereed Multi-Prover



Refereed Multi-Prover



Rational
Refereed Multi-Prover