black hat ASIA 2025

APRIL 3-4, 2025
BRIEFINGS

The ByzRP Solution

A Global Operational Shield for RPKI Validators

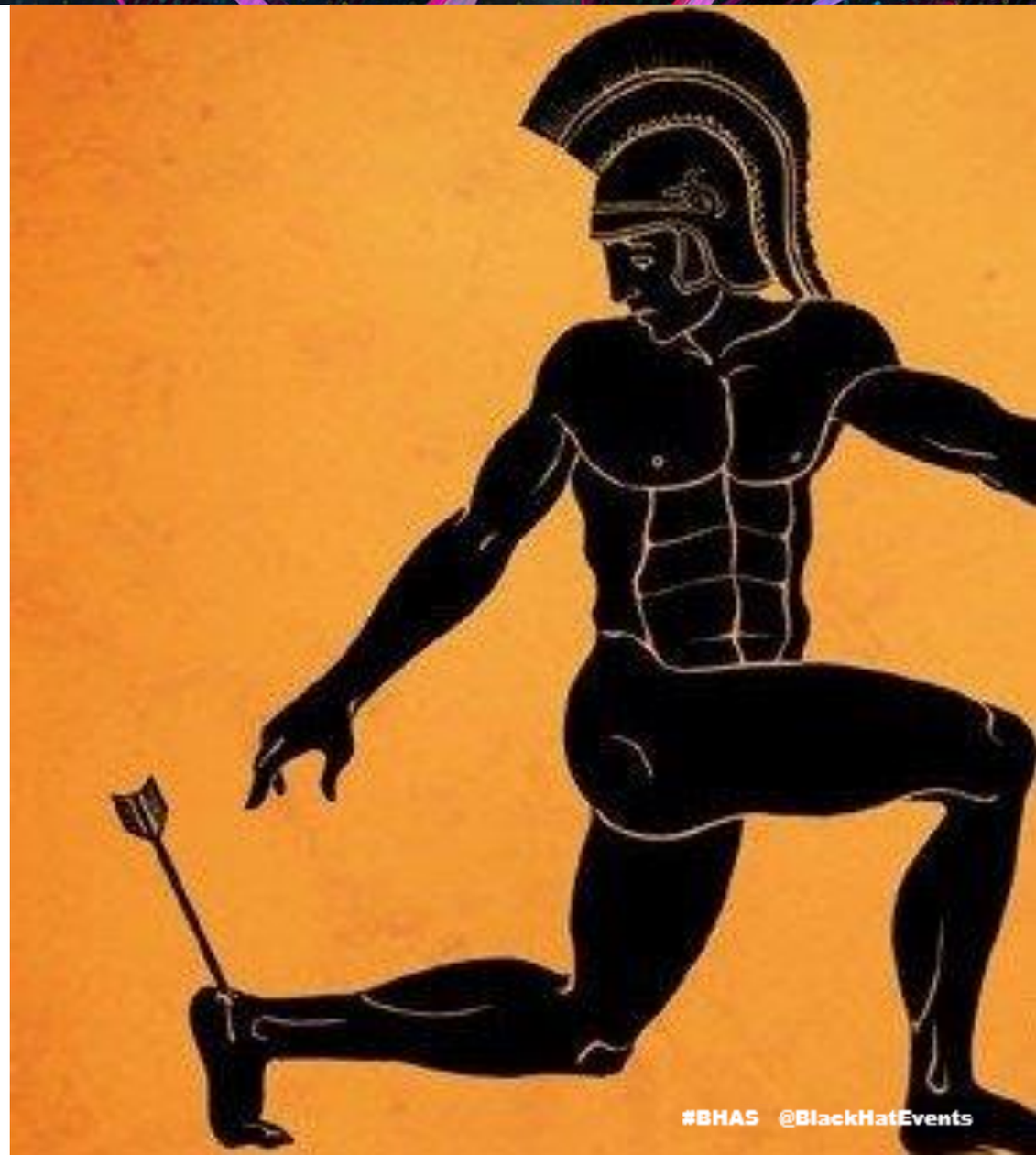
Jens Friess | Donika Mirdita | Haya Schulmann | Michael Waidner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

BGP
The Achilles' Heel of the Internet



B.G.P.

Boundary Gateway Protocol

block length — 2 bytes
version number — 1 byte
block type — 1 byte (reserved, must)
holddown timer — 2 bytes (minutes)

types:
- open - 1
- update - 2
- notification - 3
- keepalive - 8

version is currently 1

open:
- my AS # — 2 byte
- link type — 1 byte
  - up - 1
  - down - 2
  - internal - 4
  - H-link - 8

(not used in update direction field)

- auth type code — 1 byte
  - 0 - none
- authentication — variable

update:

repeat structure according to block length

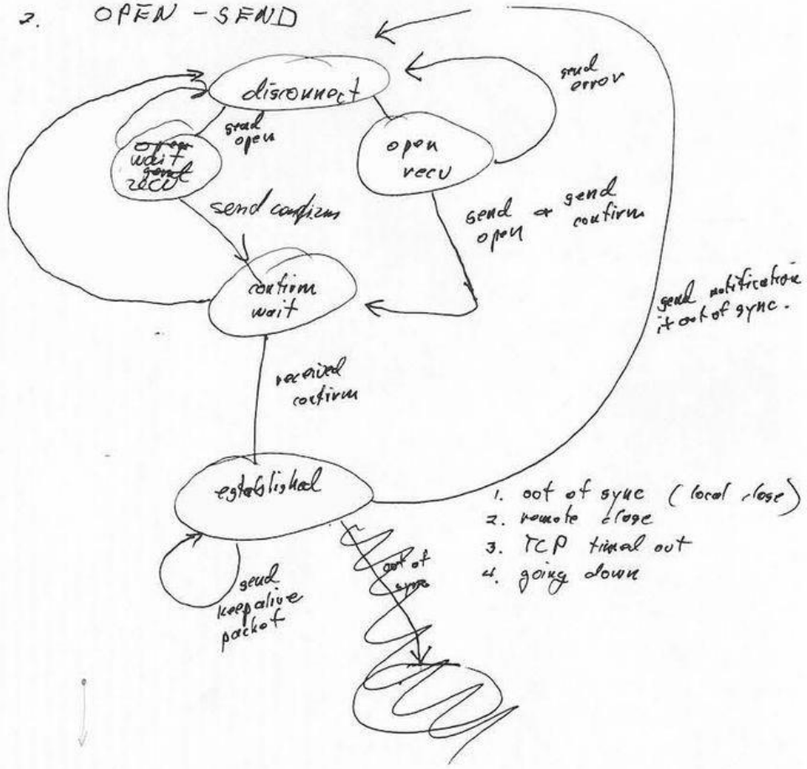
- network # — 4 bytes
- first hop gateway — 4 bytes
- metric — 2 bytes
- count of AS — 1 byte
- {direction — 1 byte
- {AS # — 2 byte

} repeat "count" times

notification:
- oprode — 2 bytes
- data — variable

State Diagram

1. initial state is DISCONNECT
2. OPEN - SEND



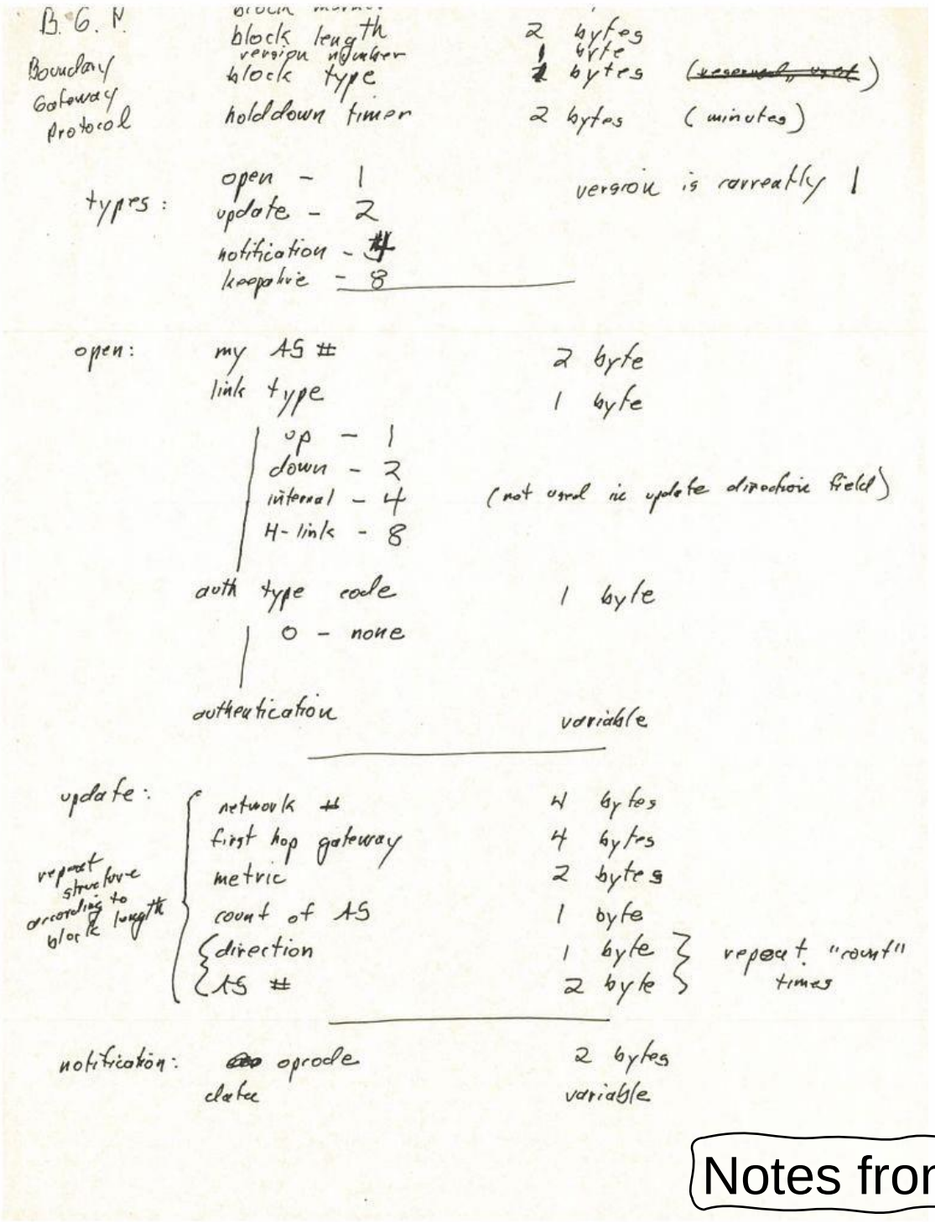
loughheed@cisco.com 415-326-1941 (11-7) PST
YAKOV@IBM.COM (914)945-3896 (8-5) EST

Border Gateway Protocol (BGP) is the defacto inter-domain routing protocol.

It prioritizes:

- **Scalability**
- **Efficiency**
- **Speed**

Notes from the IETF Cafeteria, 1989



B.G.P.

Boundary Gateway Protocol

block length — 2 bytes
version number — 1 byte
block type — 1 byte (reserved, must)
holddown timer — 2 bytes (minutes)

types:
- open - 1
- update - 2
- notification - 3
- keepalive - 8

version is currently 1

open:
- my AS # — 2 byte
- link type — 1 byte
  - up - 1
  - down - 2
  - internal - 4
  - H-link - 8

(not used in update direction field)

- auth type code — 1 byte
  - 0 - none
- authentication — variable

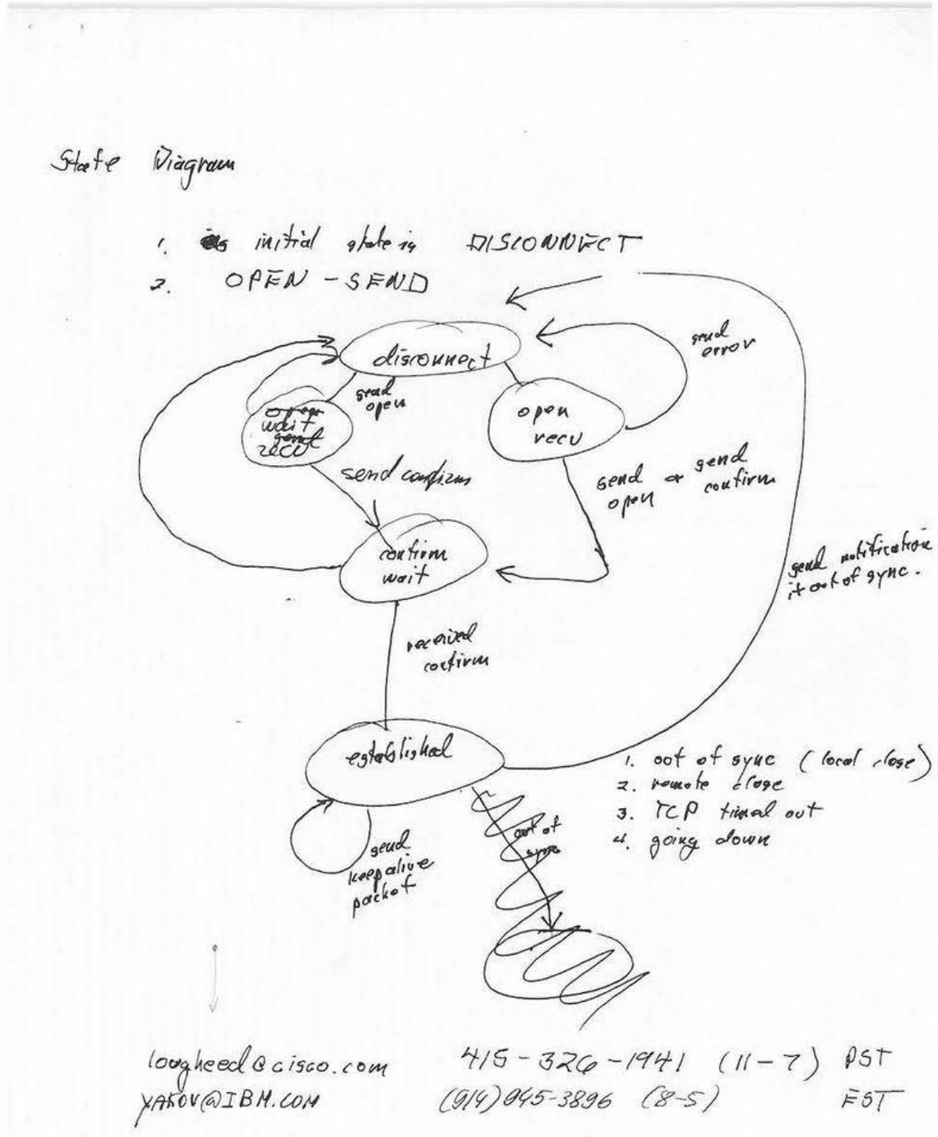
update:

repeat structure according to block length

- network # — 4 bytes
- first hop gateway — 4 bytes
- metric — 2 bytes
- count of AS — 1 byte
- direction — 1 byte
- AS # — 2 byte

repeat "count" times

notification:
- oprode — 2 bytes
- data — variable



loughheed@cisco.com 415-326-1941 (11-7) PST
YAKOV@IBM.COM (914)945-3896 (8-5) EST

Notes from the IETF Cafeteria, 1989

Border Gateway Protocol (BGP) is the defacto inter-domain routing protocol.

It prioritizes:

- ❖ **Scalability**
- ❖ **Efficiency**
- ❖ **Speed**
- ❖ ~~**Security**~~

Long History of BGP Routing Hijacks...

OUTAGE ANALYSES

Twitter Outage Analysis: March 28, 2022

By Chris Villemez | April 15, 2022 | 14 min read

ROUTING SECURITY INCIDENTS

For 12 Hours, Was Part of Apple Engineering's Network Hijacked by Russia's Rostelecom?

By Aftab Siddiqui • 27 Jul 2022

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.

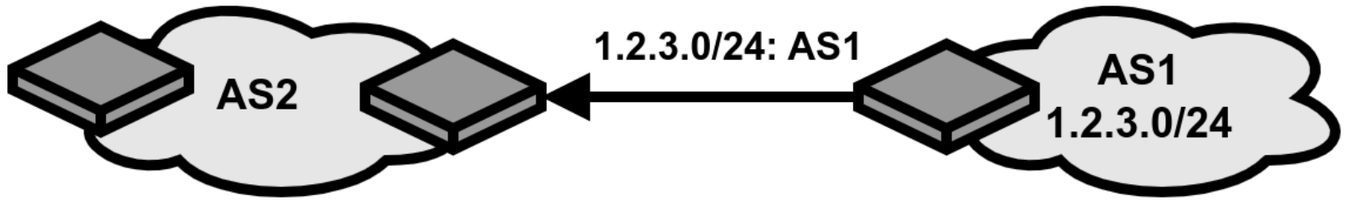
Written by **Catalin Cimpanu,** Contributor

April 5, 2020 at 2:53 p.m. PT

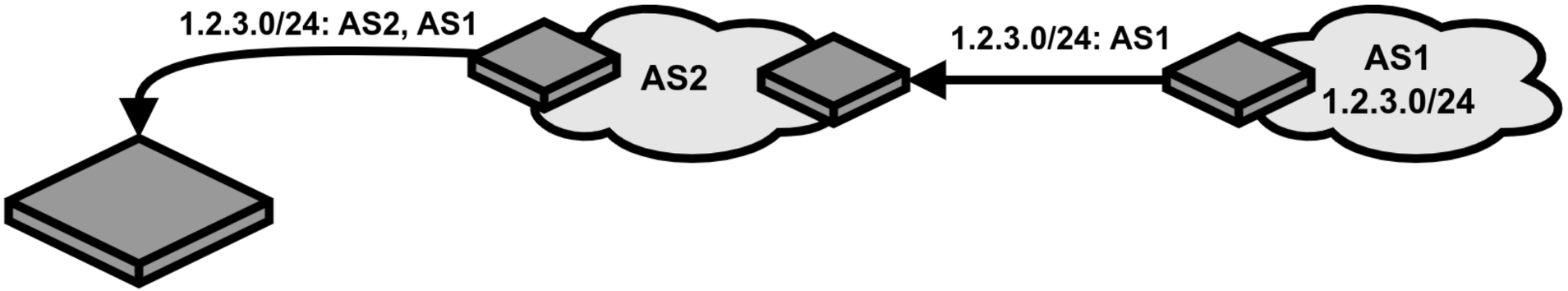
Cloudflare blames recent outage on BGP hijacking incident

By **Bill Toulas** July 5, 2024 02:41 PM 1

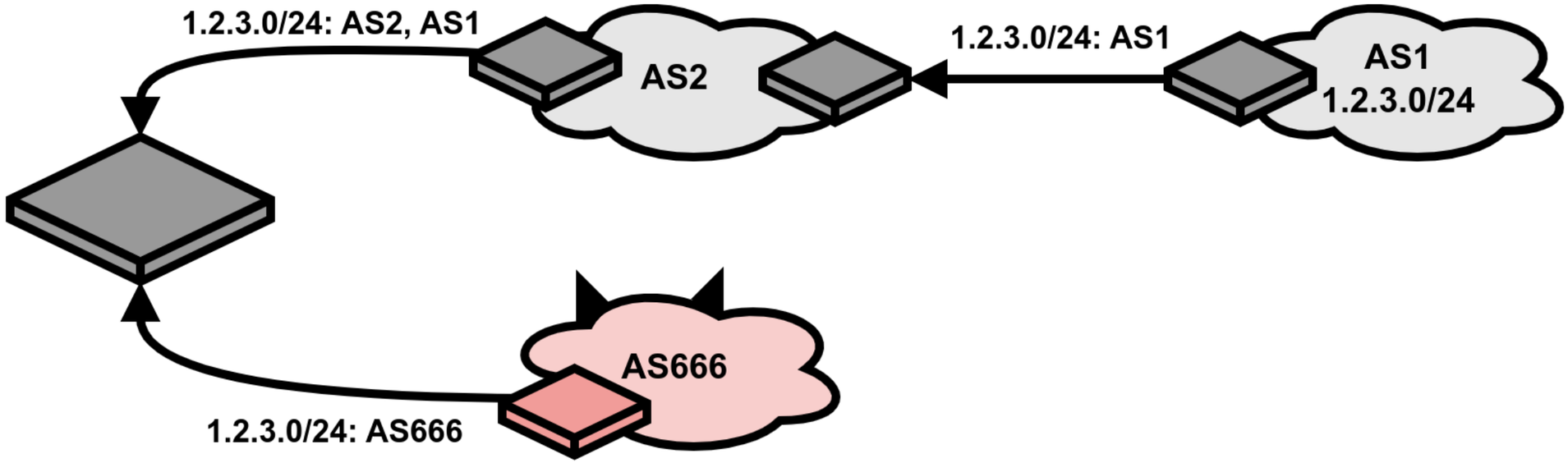
BGP Route Announcement



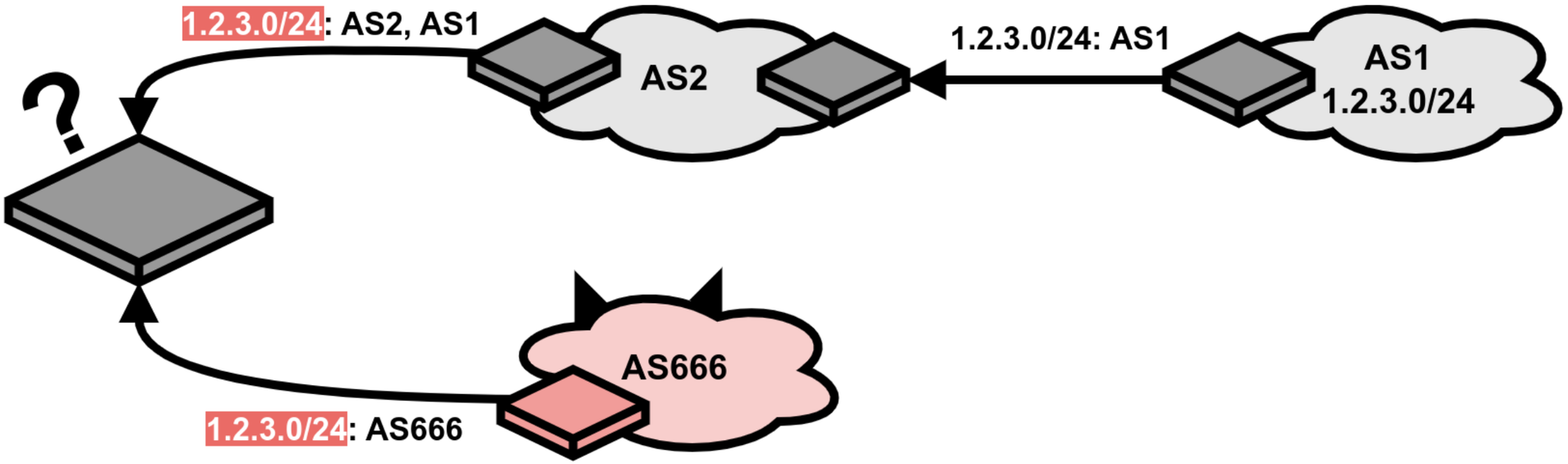
Forwarding Neighboring Announcement



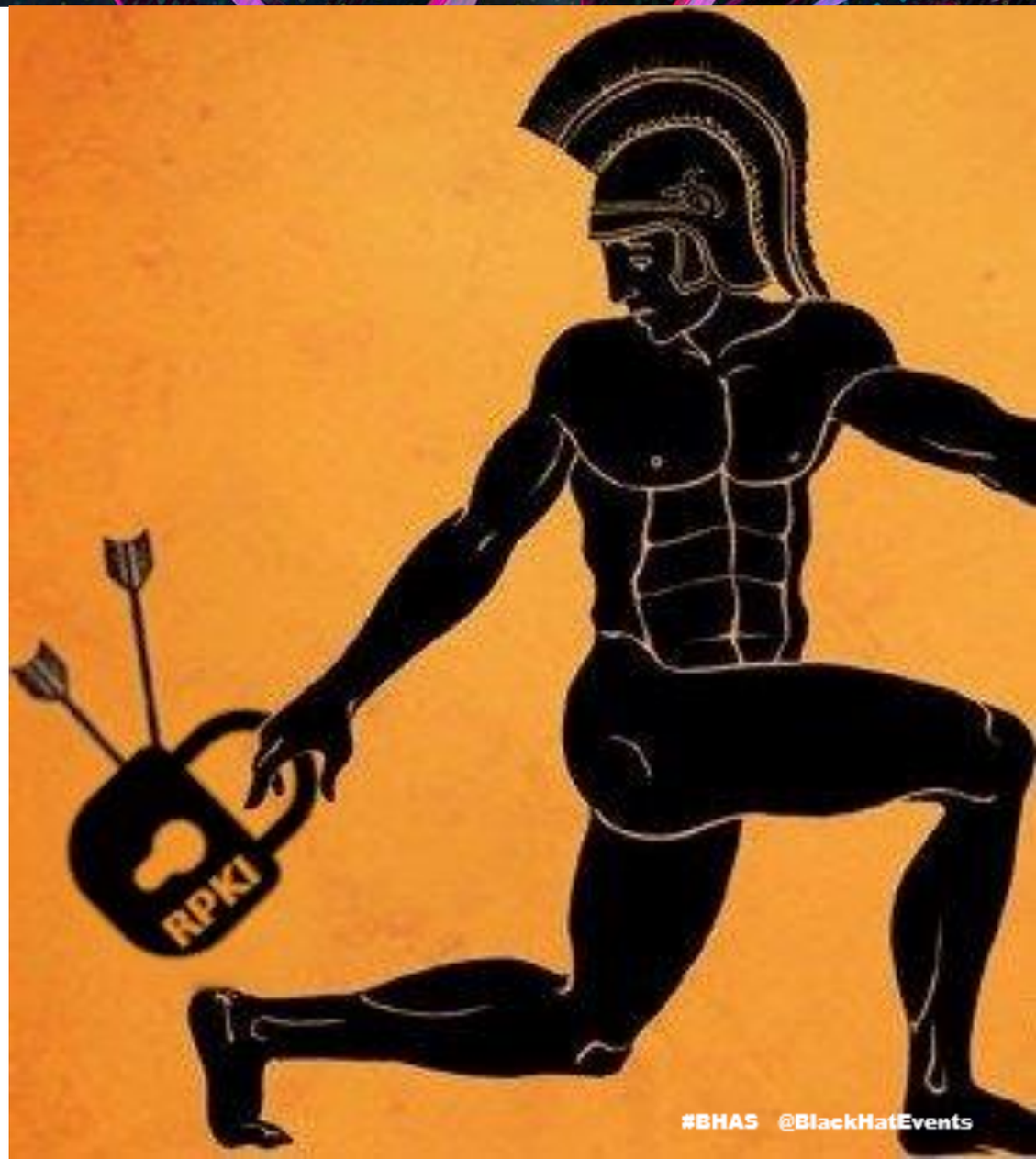
BGP Prefix Hijack



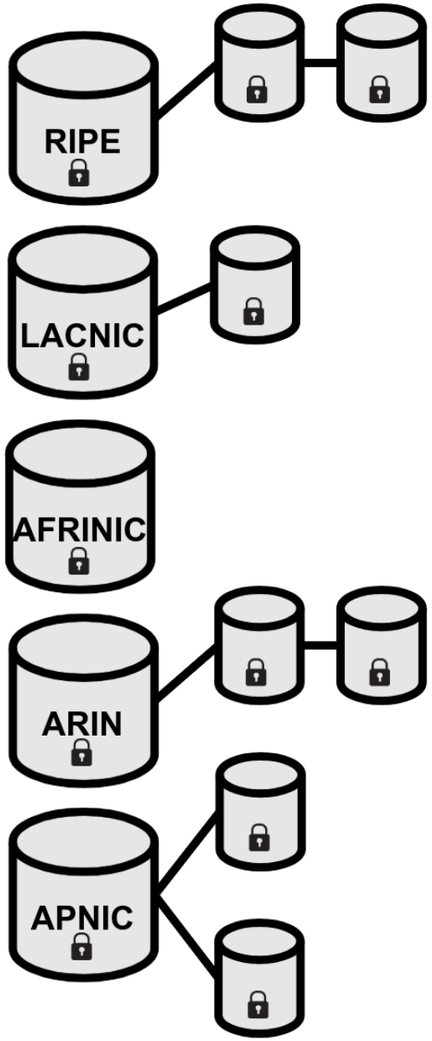
BGP Prefix Hijack



RPKI
Resource Public Key Infrastructure

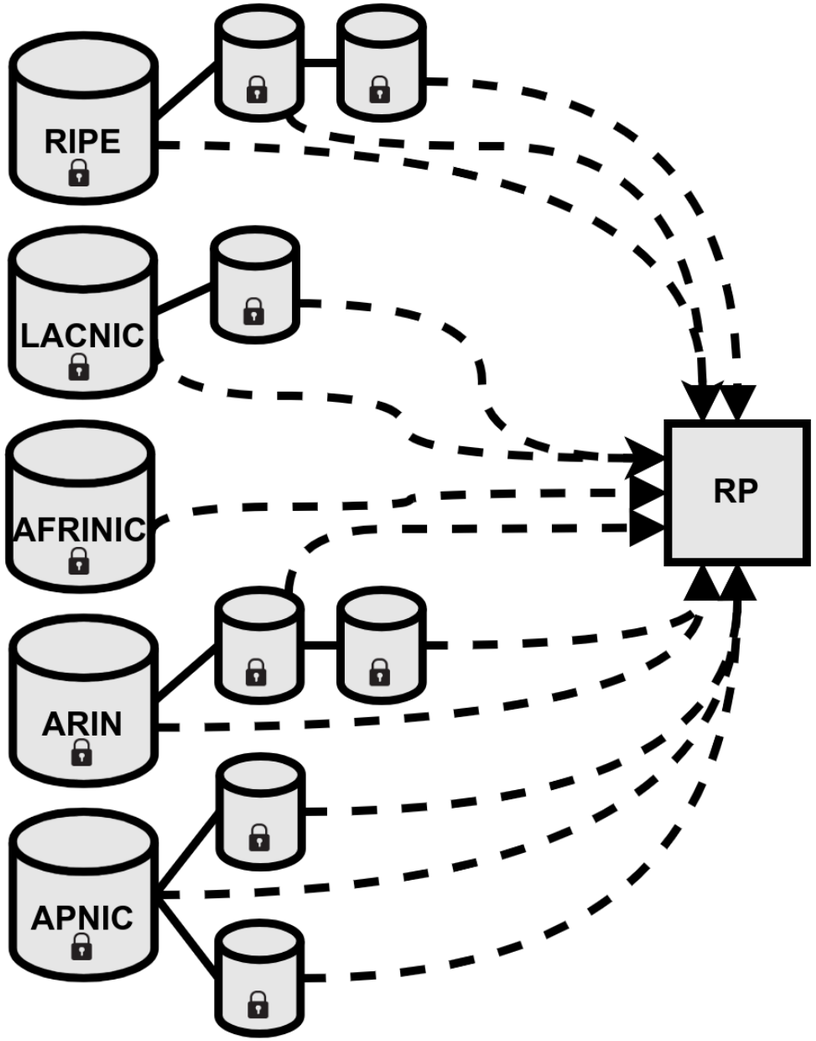


RPKI: Cryptographic Objects in *Publication Points*



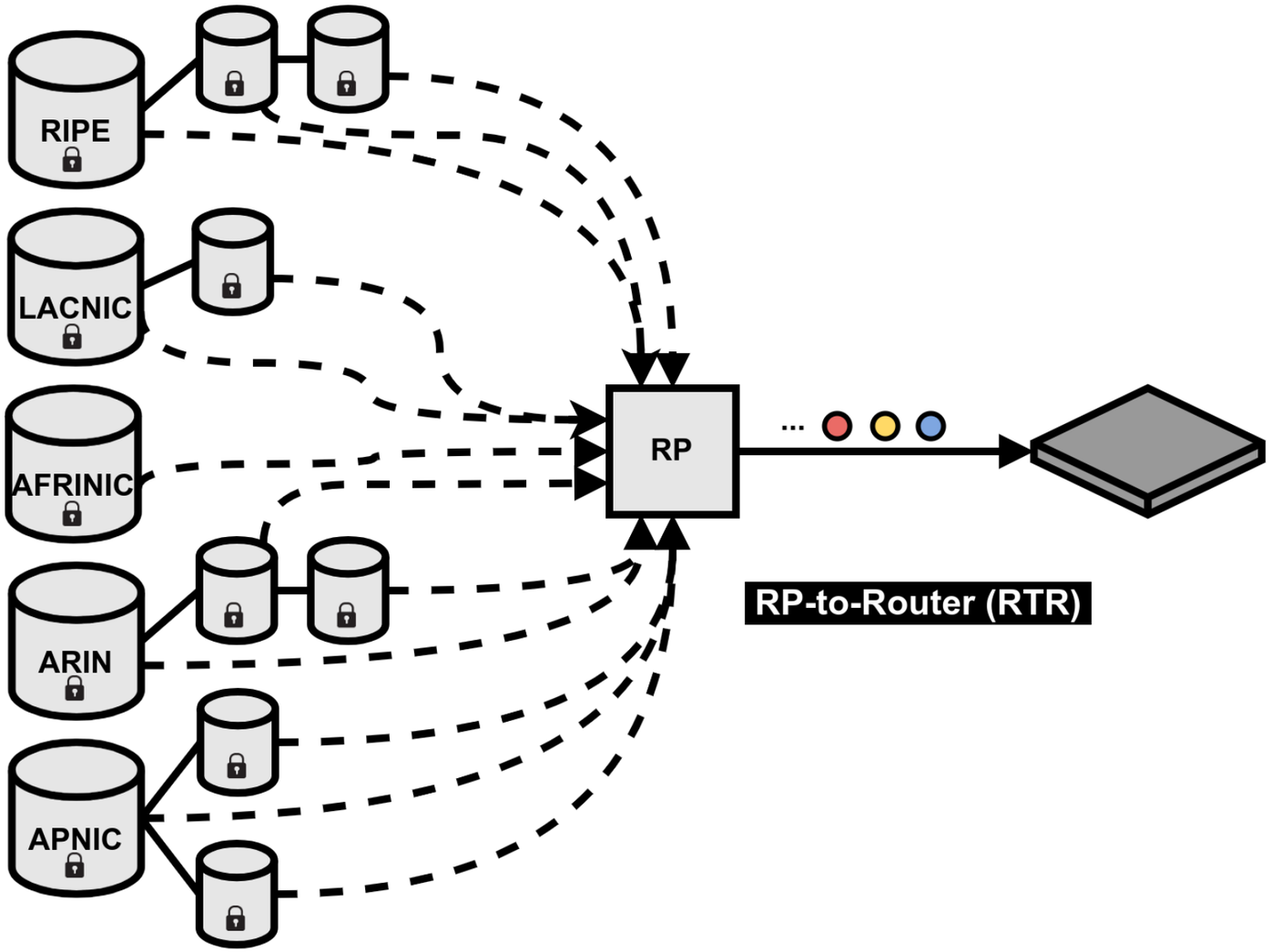
Publication Point Repository Tree

RPKI: Objects Collected by *Relying Party*



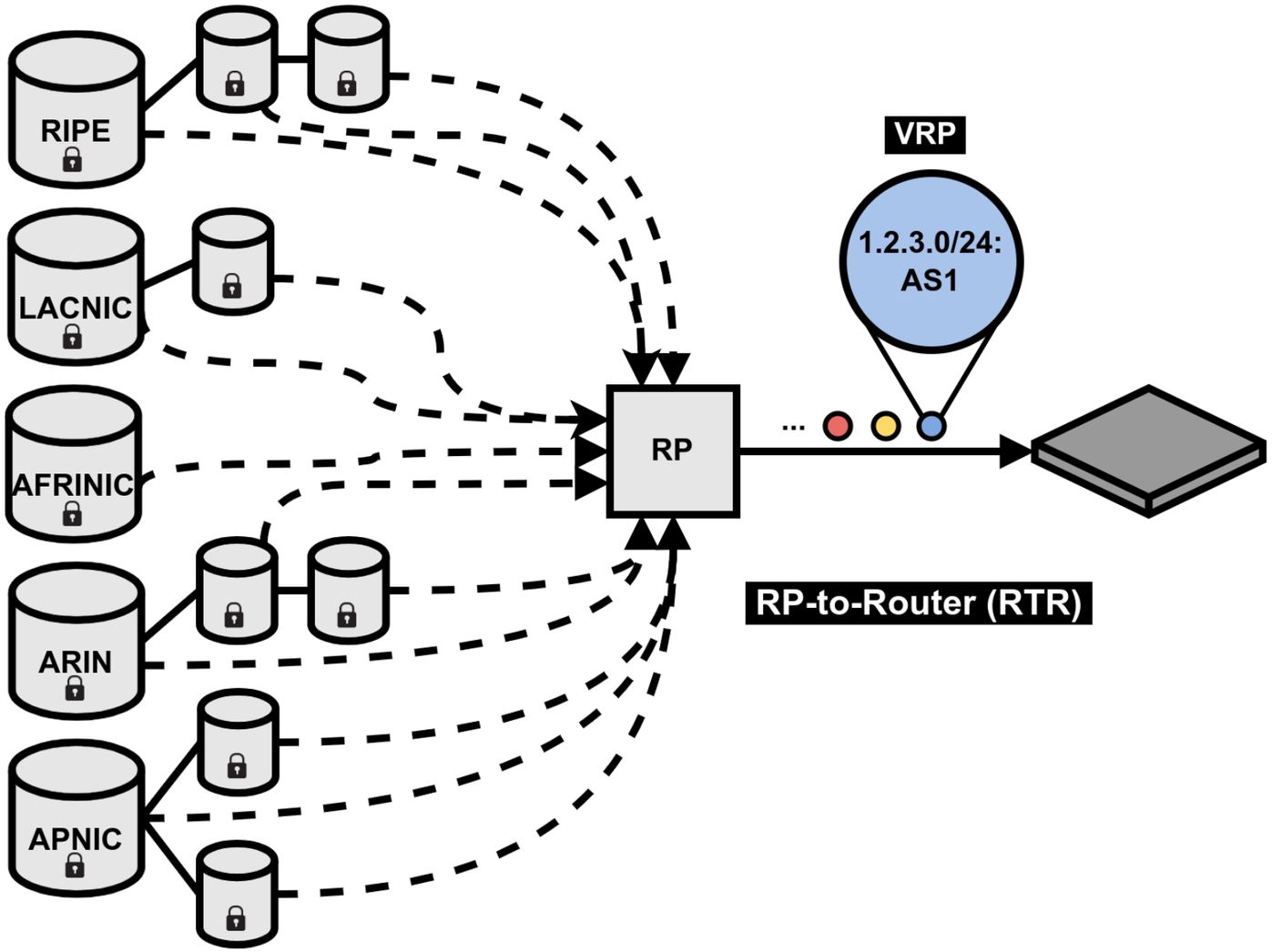
Publication Point Repository Tree

RPKI: Validated Objects Sent to Router



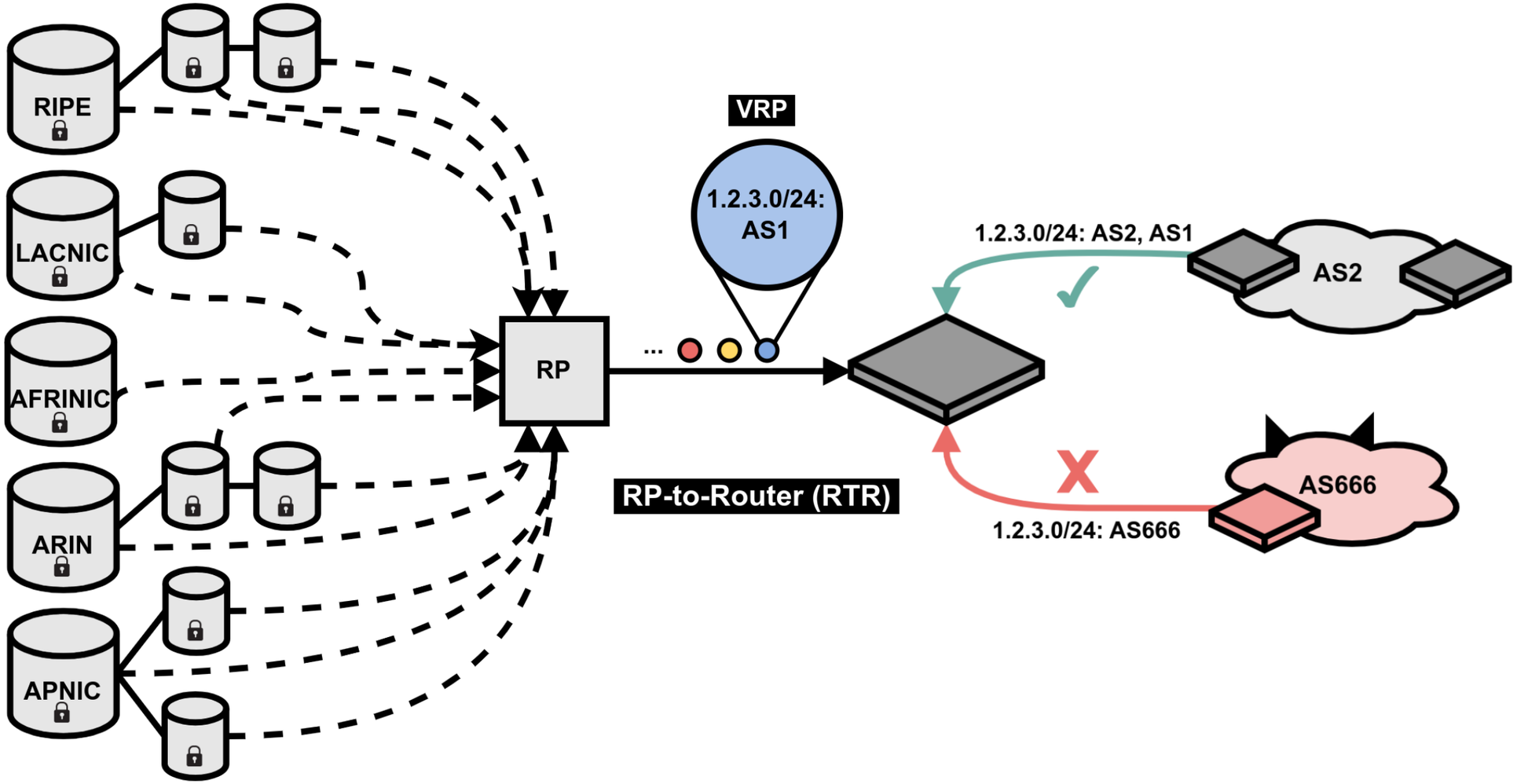
Publication Point Repository Tree

RPKI: *Validated ROA Payloads (VRPs)*



Publication Point Repository Tree

RPKI: VRPs to Verify BGP Announcements



Publication Point Repository Tree

RPKI - the most promising BGP security add-on

Capacity Media

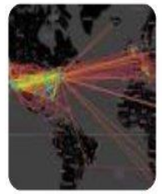
Telia Carrier set to install RPKI to global backbone

Telia Carrier has announced that it will be implementing resource public key infrastructure (RPKI) technology to its global network.

17 Sept 2019

BleepingComputer

Comcast now blocks BGP hijacking attacks and route leaks with RPKI



Comcast, one of America's largest broadband providers, has now deployed RPKI on its network to defend against BGP route hijacks and leaks.

20 May 2021

How AWS is helping to secure internet routing

by Fredrik Korsbäck | on 13 JAN 2021 | in Announcements, Best Practices, Networking & Content Delivery,

Verisign's Path to RPKI

By Mike Hollyman • 7 Jun 2023

case study RPKI

BGP HIJACKING —

FCC pushes ISPs to fix security flaws in Internet routing

Chair: Addressing BGP flaws will "help make our Internet routing more secure."

JON BRODKIN - 6/6/2024, 11:40 PM

BleepingComputer

All Dutch govt networks to use RPKI to prevent BGP hijacking

The Dutch government will adopt the RPKI (Resource Public Key Infrastructure) standard on all its systems before the end of 2024 to upgrade...

9 Apr 2023

RPKI - the most promising BGP security add-on

Capacity

Telia Car

Telia Carrier infrastructur

17 Sept 201

The Register®

FCC takes some action against notorious BGP

How's your RPKI-based security plan coming along? Feds want to know

Jessica Lyons

Fri 7 Jun 2024 // 22:29 UTC

How A

by Fredrik Korsbäck | on 13 JAN 2021 | in Announcements, Best Practices, Networking & Content Delivery,

Verisign's Path to RPKI

By Mike Hollyman • 7 Jun 2023

case study RPKI

BGP HIJACKING —

FCC pushes ISPs to fix security flaws in Internet routing

Chair: Addressing BGP flaws will "help make our Internet routing more secure."

JON BRODKIN - 6/6/2024, 11:40 PM

BleepingComputer

All Dutch govt networks to use RPKI to prevent BGP hijacking

The Dutch government will adopt the RPKI (Resource Public Key Infrastructure) standard on all its systems before the end of 2024 to upgrade...

9 Apr 2023

Capacity

Telia Car

Telia Carrier infrastructur

17 Sept 201

How A

by Fredrik Korsbäck | on 13 JAN 2021 | in Announcements, Best Practices, Networking & Content Delivery,

BGP HIJACKIN

FCC

Inter

Chair: Addi

JON BRODKIN - 6

The Register®

FCC takes some action against notorious BGP

How's your RPKI-based security plan coming along? Feds want to know

Jessica Lyons

Fri 7 Jun 2024 // 22:29 UTC

Internet Society

US Government Networks Get a Security Boost: White House Roadmap Tackles Routing Vulnerabilities

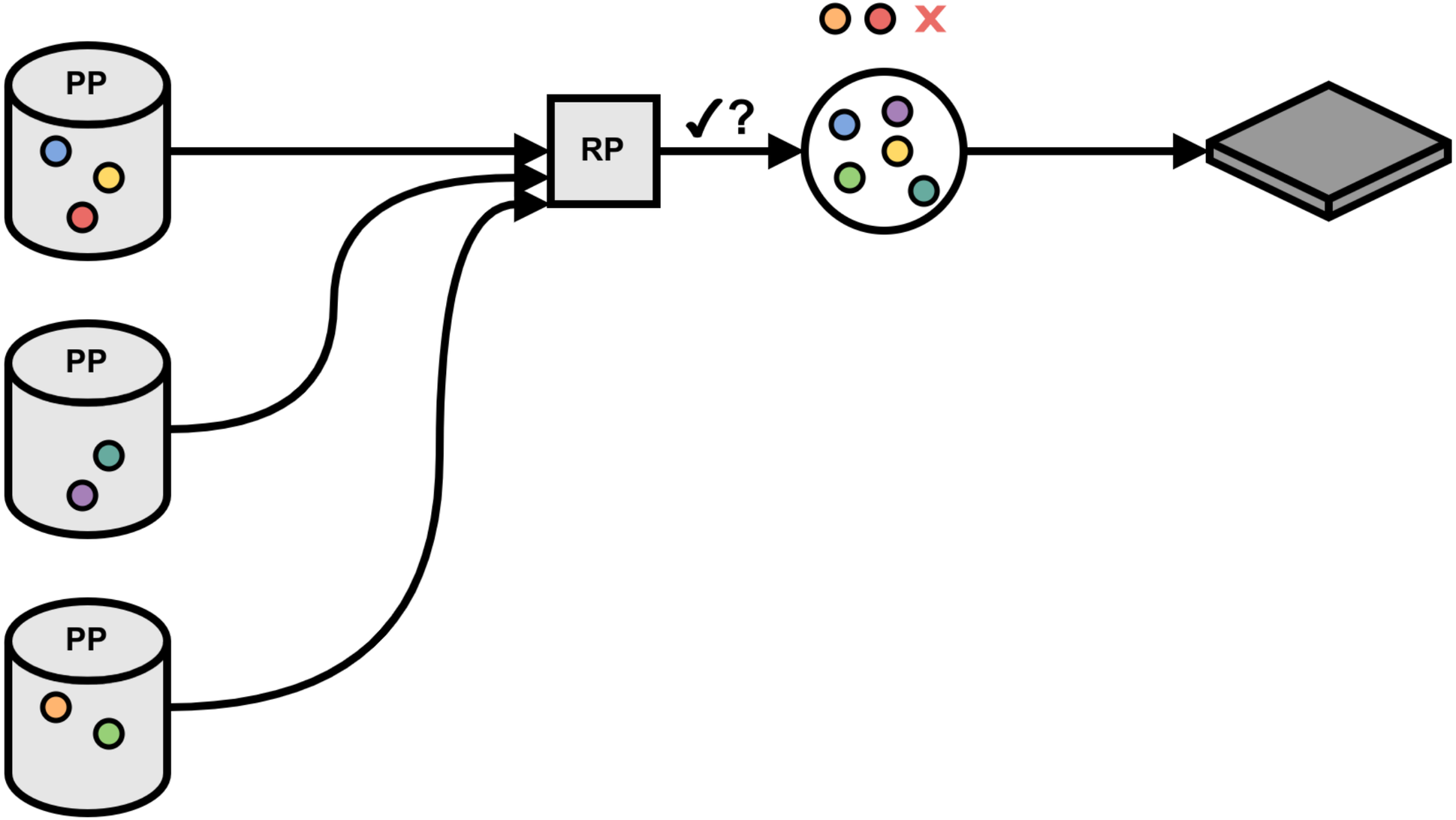
The White House's Roadmap to Enhancing Routing Security is an important step toward strengthening routing security in the United States.

06.09.2024

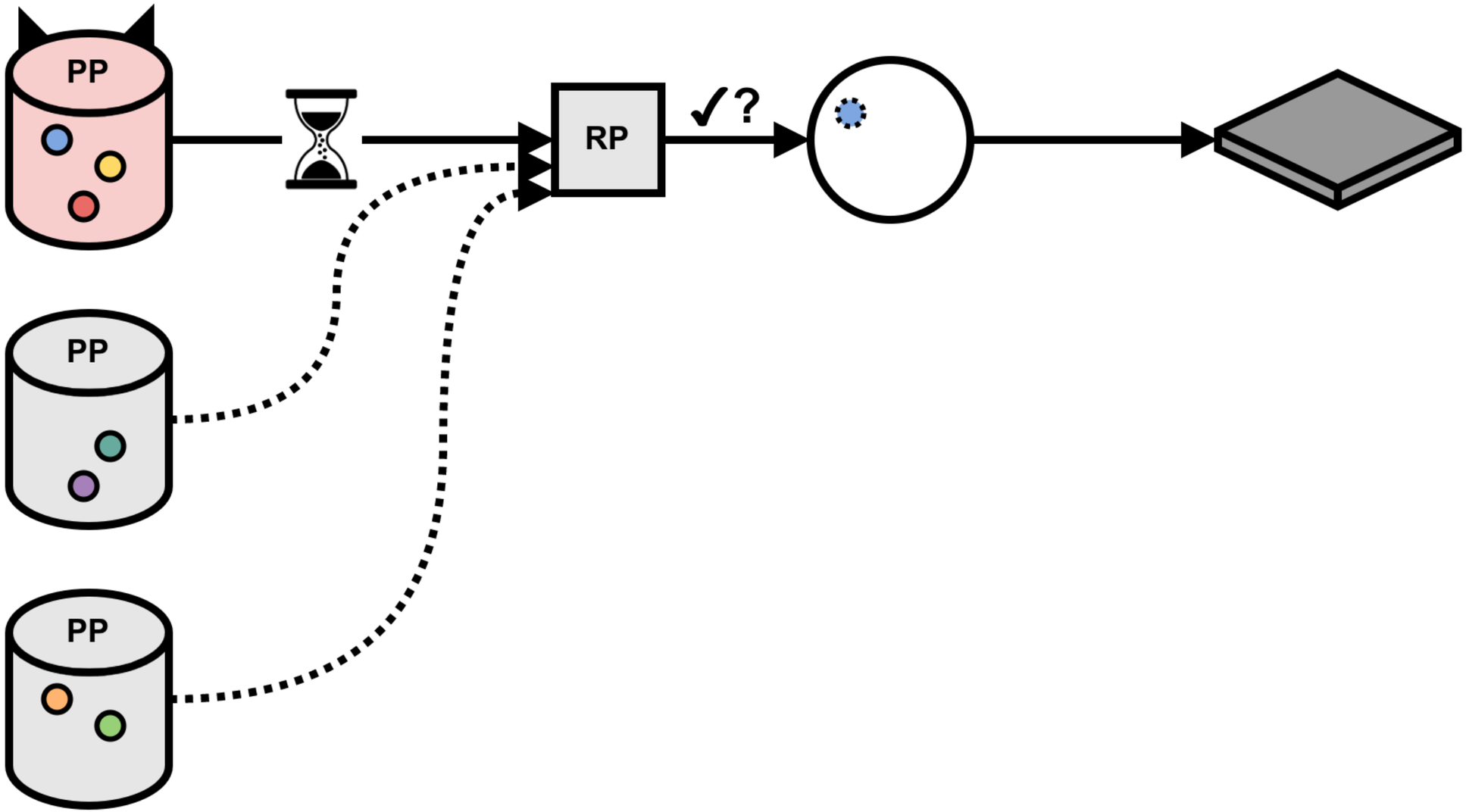
ByzRP
Operational Shield for RPKI

Malicious Publication Points
Crashing & Stalling Attacks

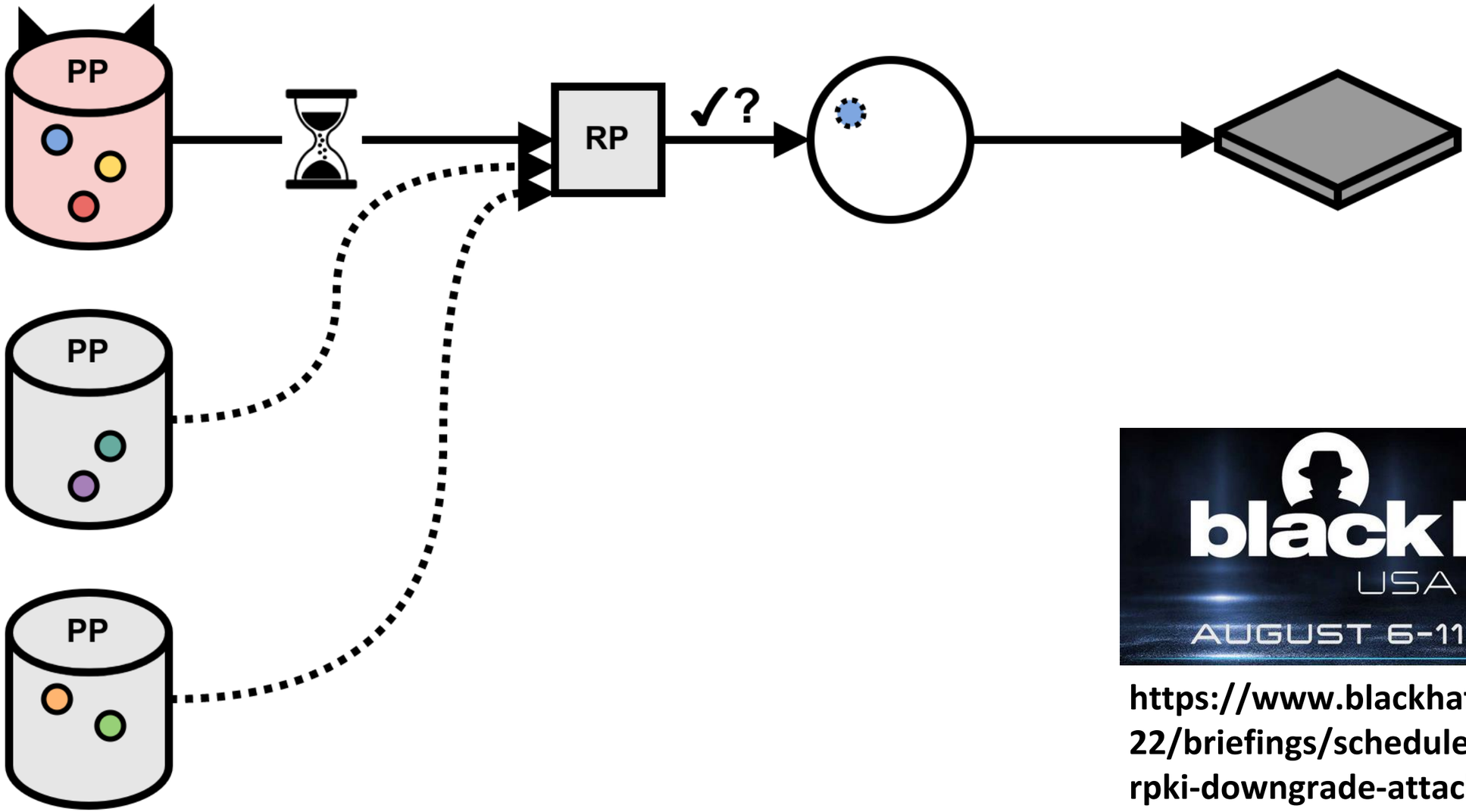
Objects Stored in Publication Points, Validated by Relying Party



Stalling Attacks

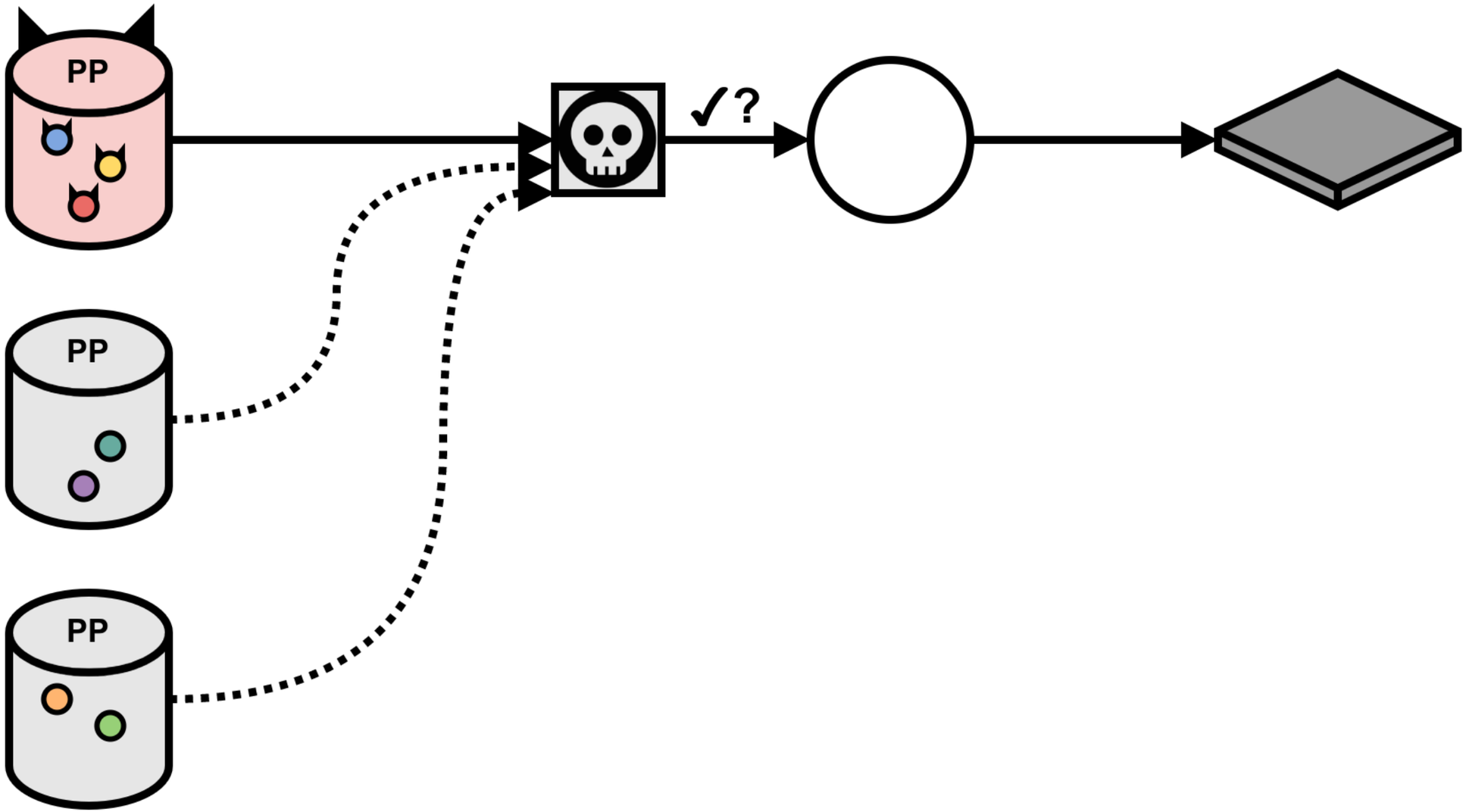


Stalling Attacks

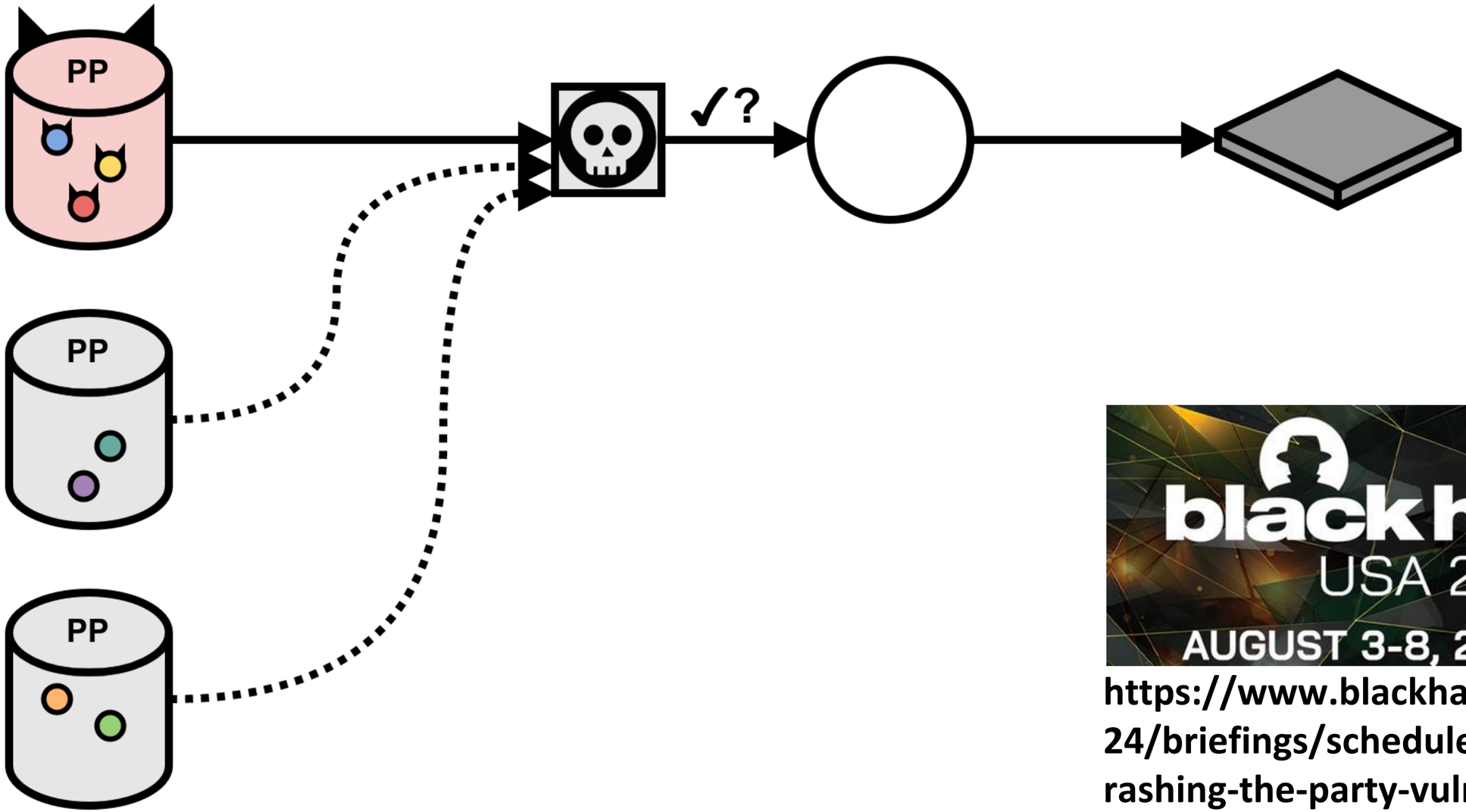


https://www.blackhat.com/us-22/briefings/schedule/#stalloris-rpki-downgrade-attack-27348

DoS Attacks

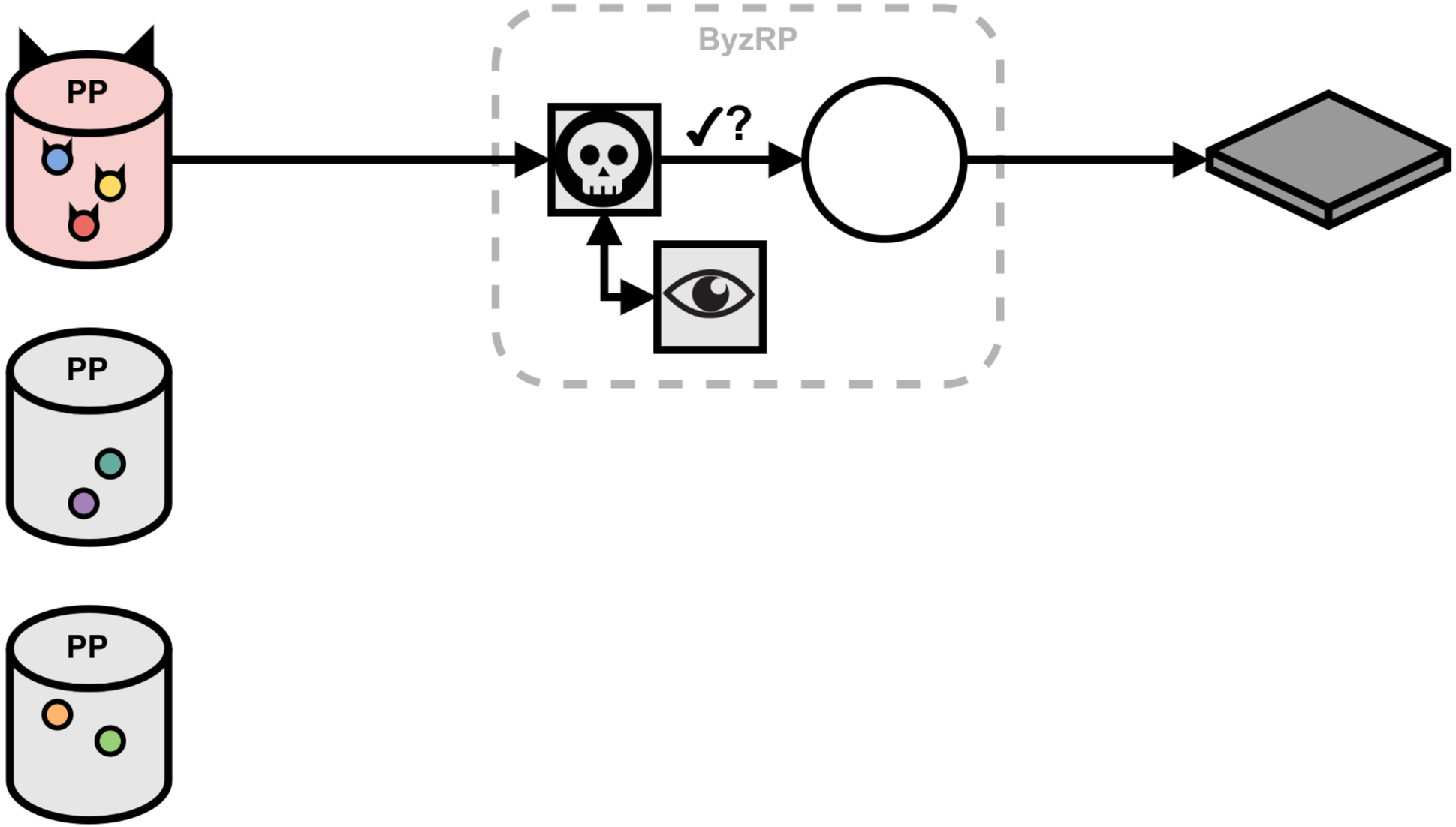


DoS Attacks

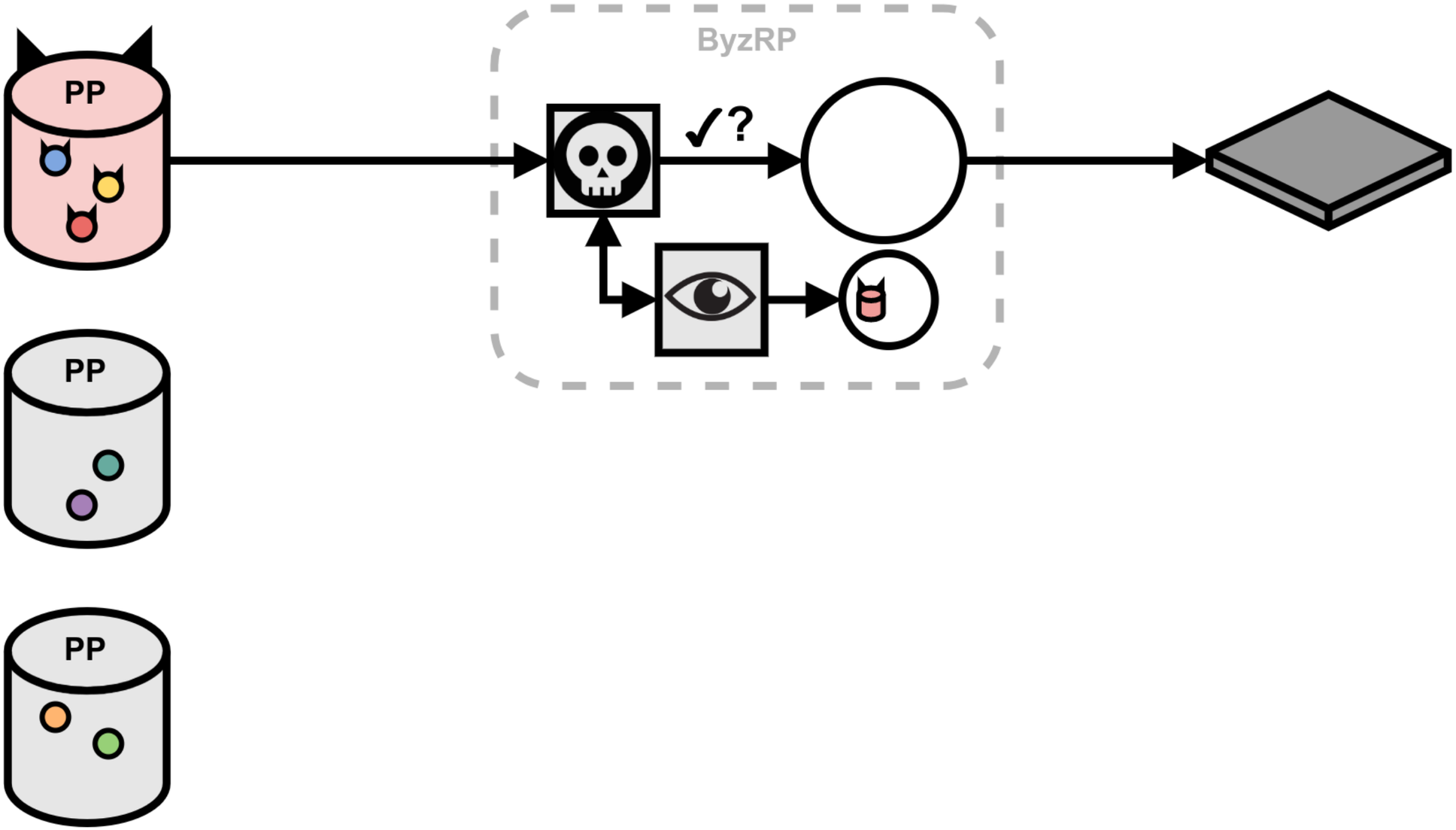


https://www.blackhat.com/us-24/briefings/schedule/index.html#crashing-the-party-vulnerabilities-in-rpki-validation-40443

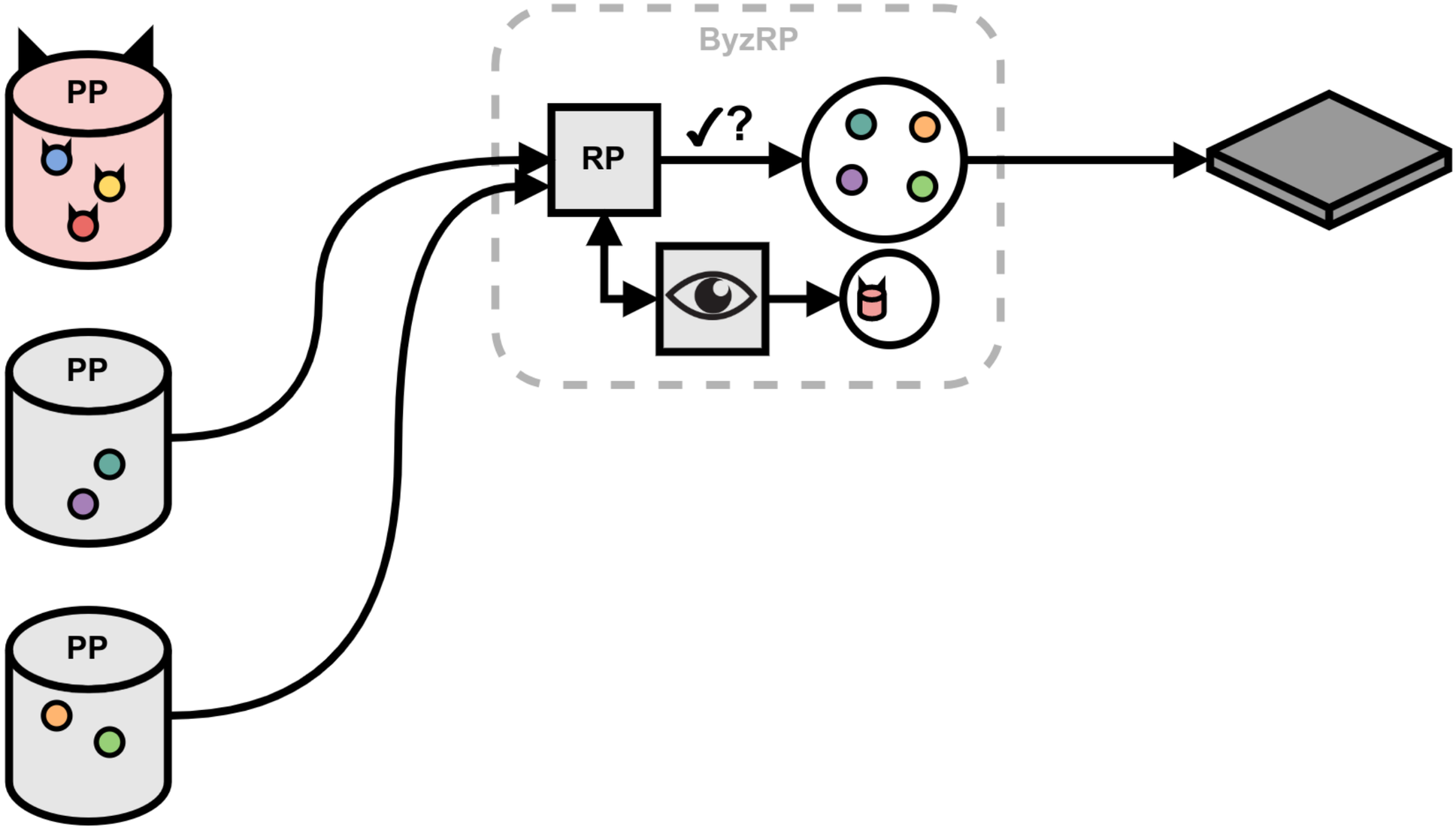
ByzRP: Watchdog



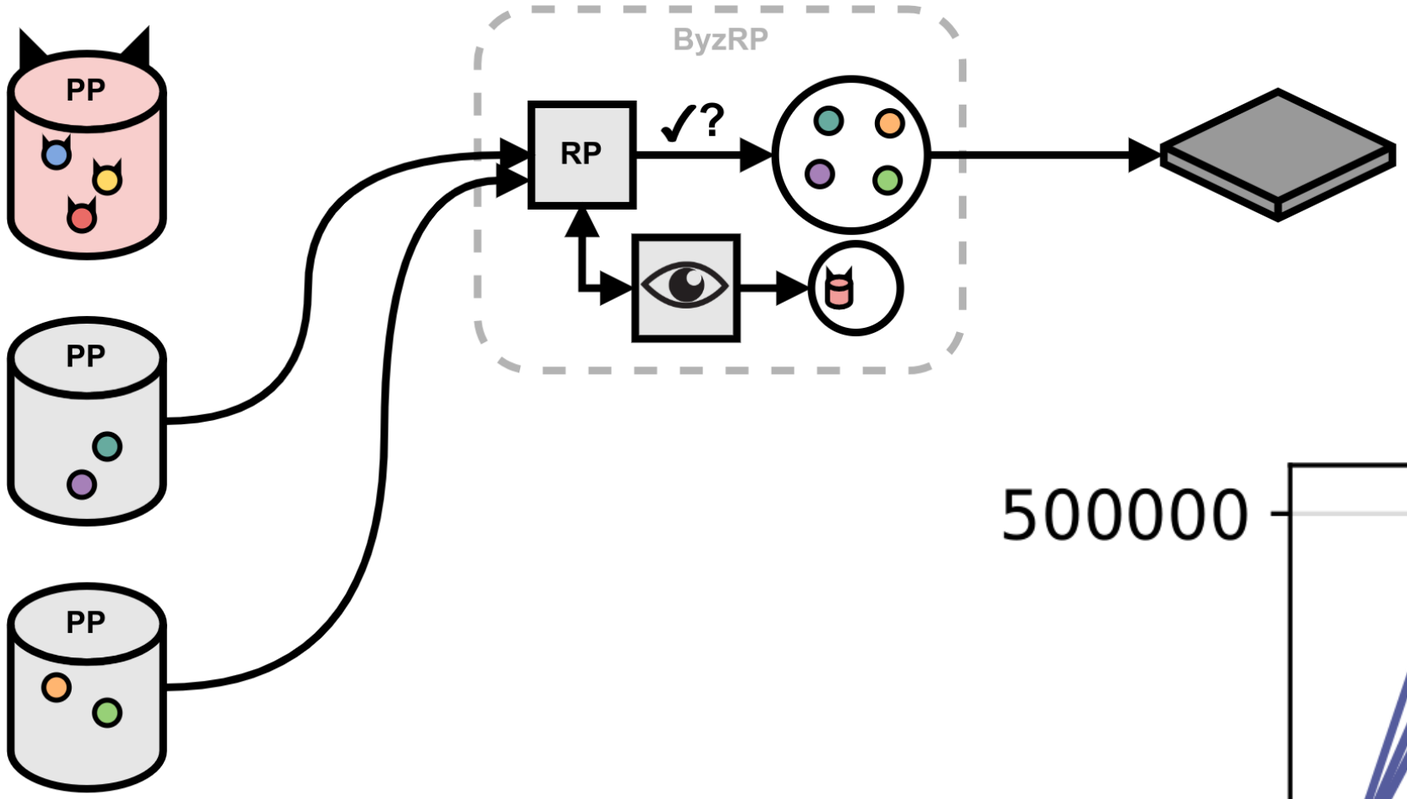
ByzRP: Watchdog

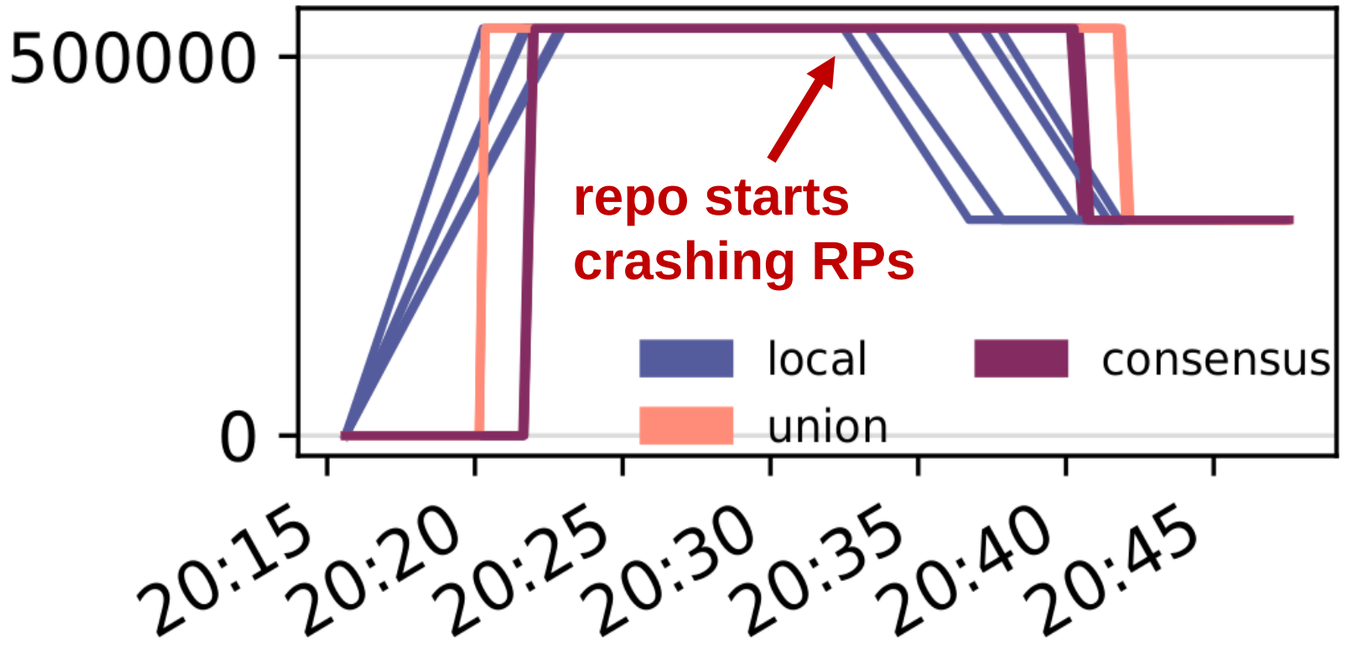


ByzRP: Watchdog

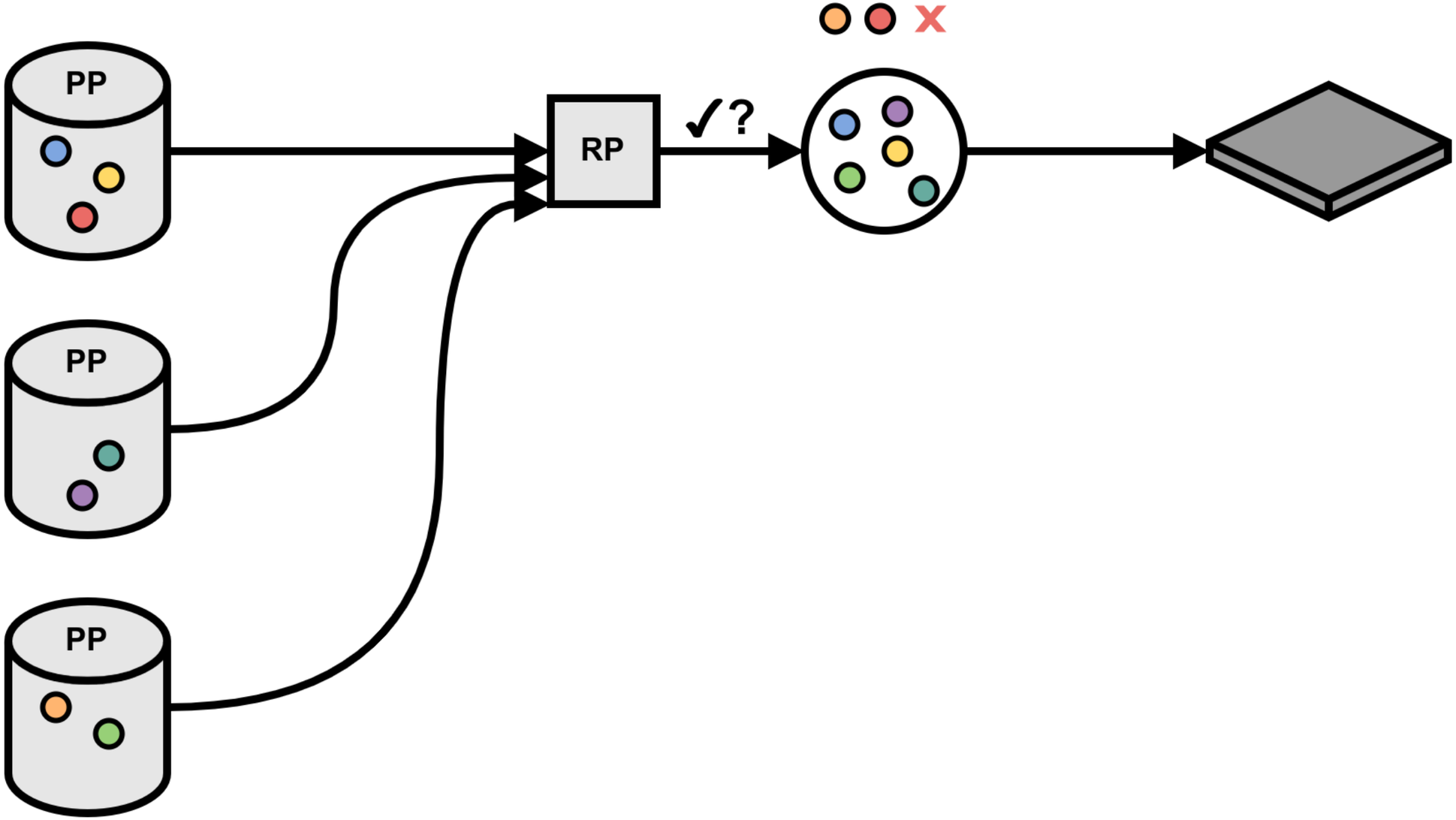


ByzRP: No Operational Downtime

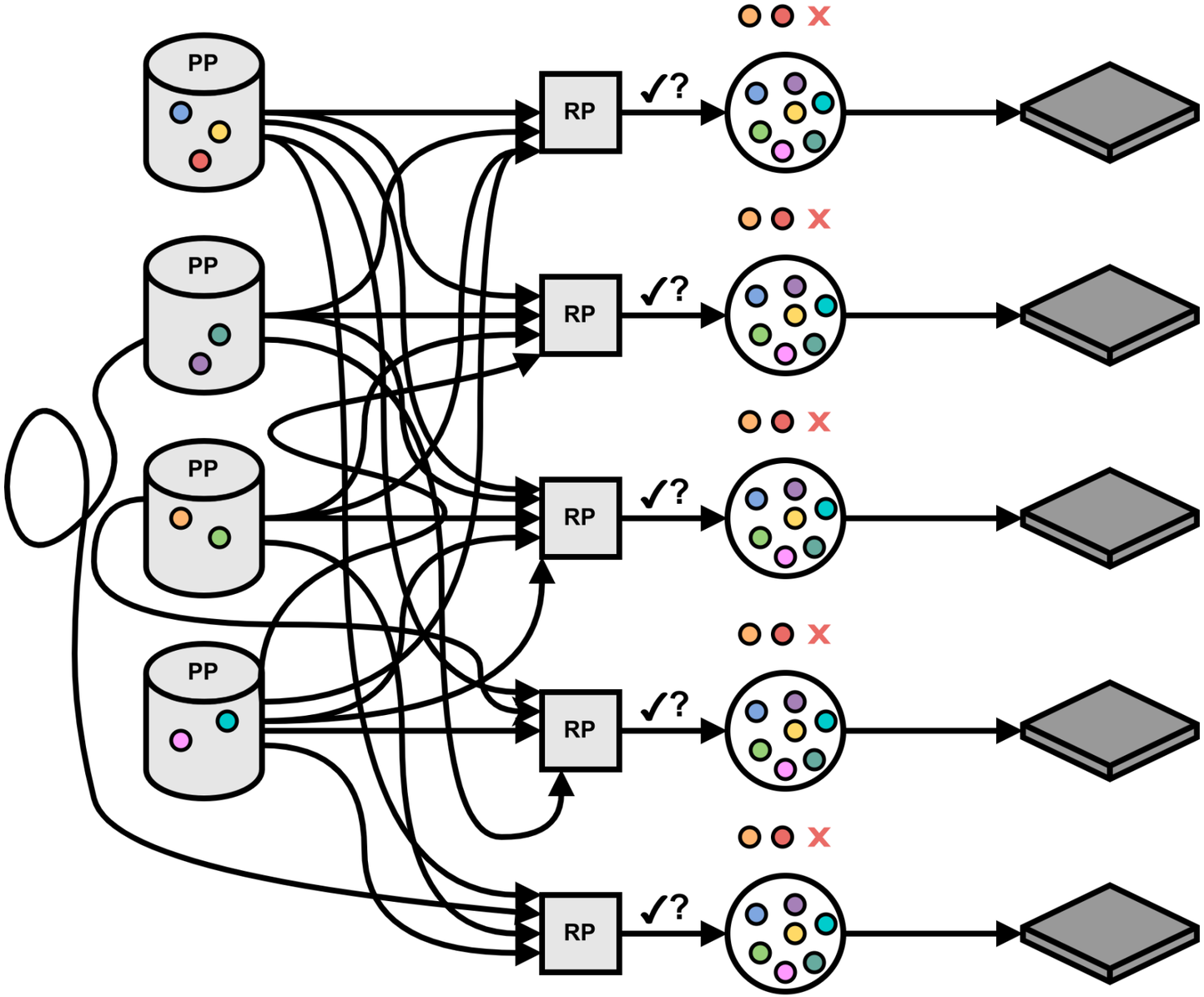




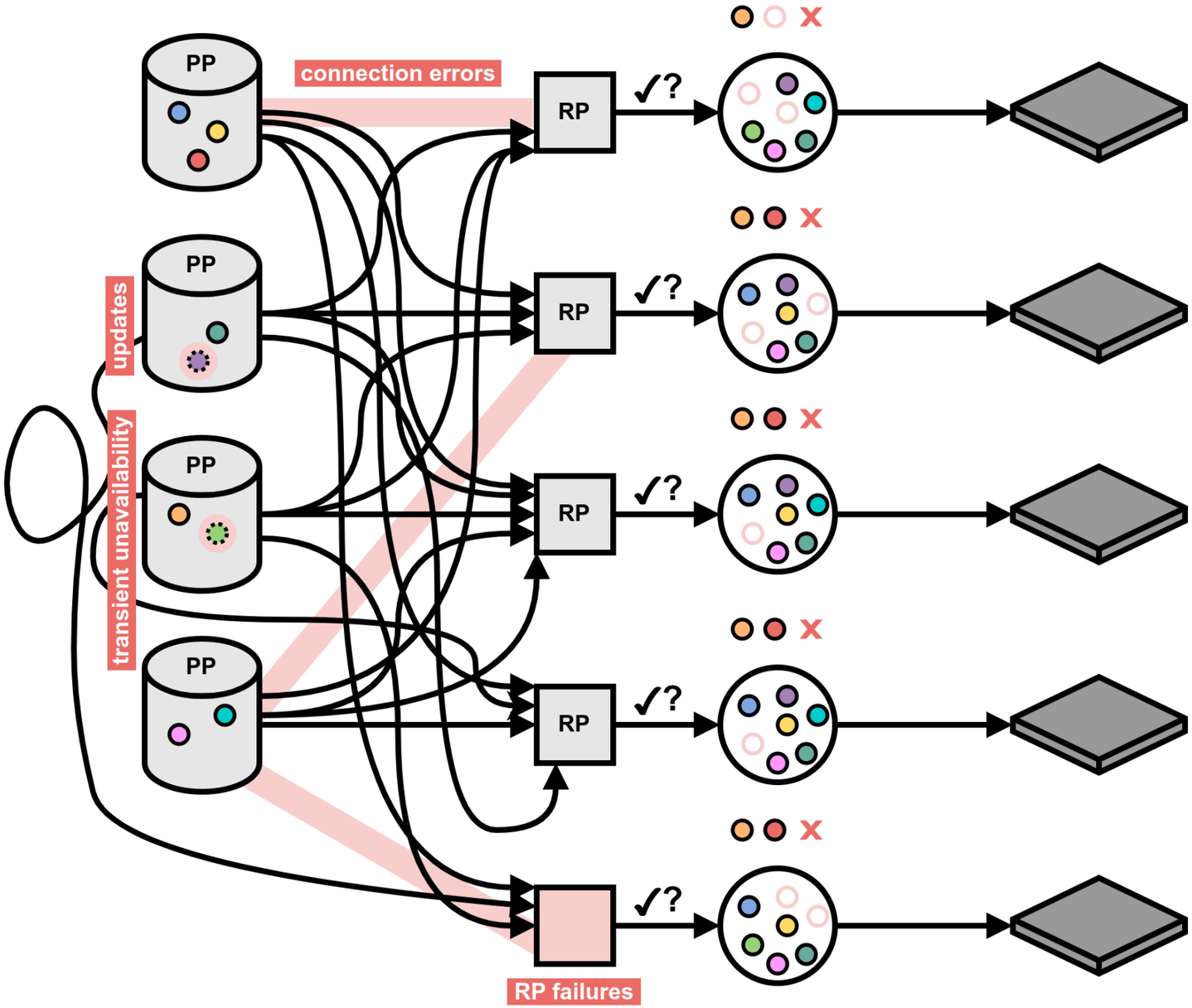
Instability
Network & Operational Errors


PP
PP
PP
RP
✓?
X

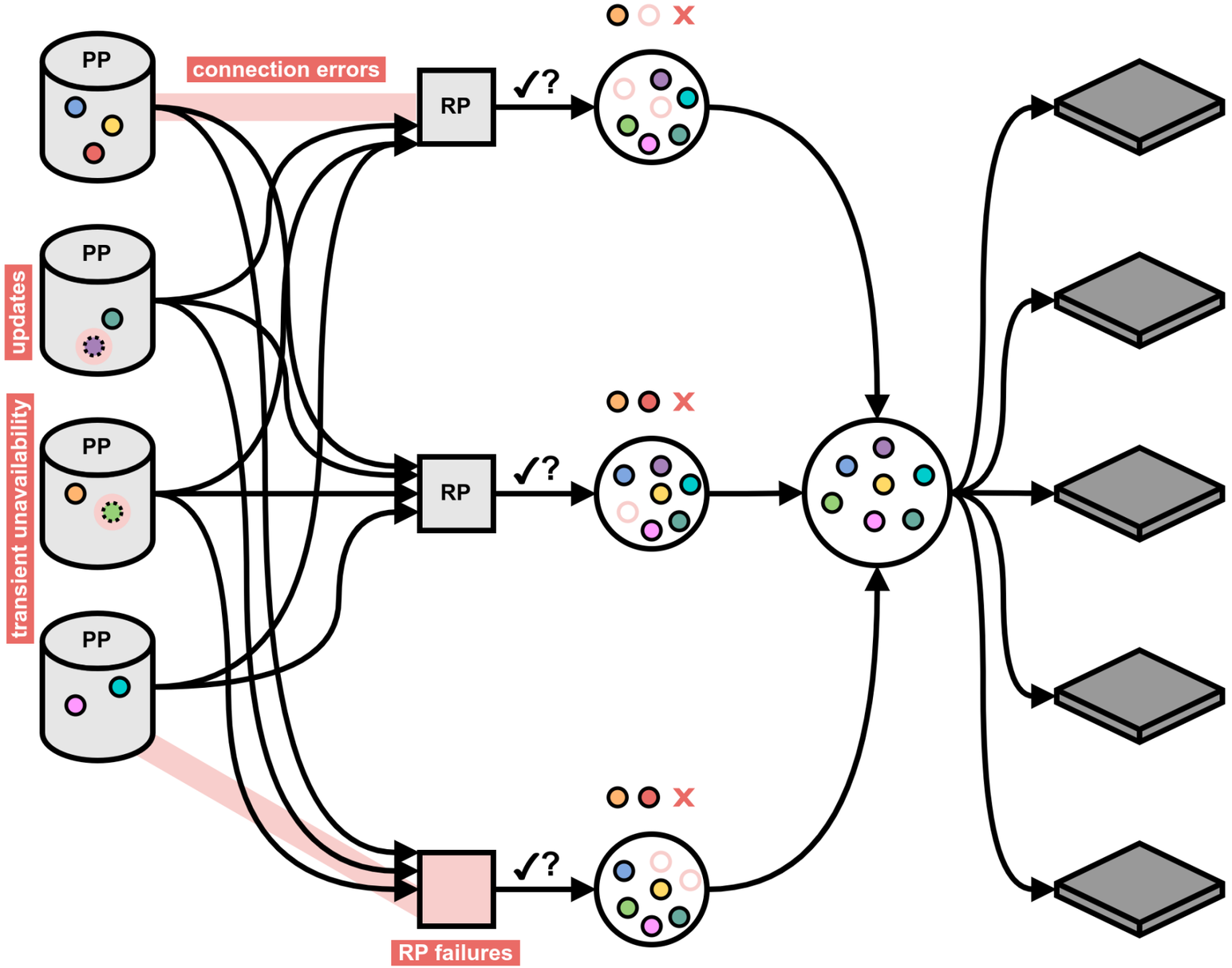
A Crowded Ecosystem



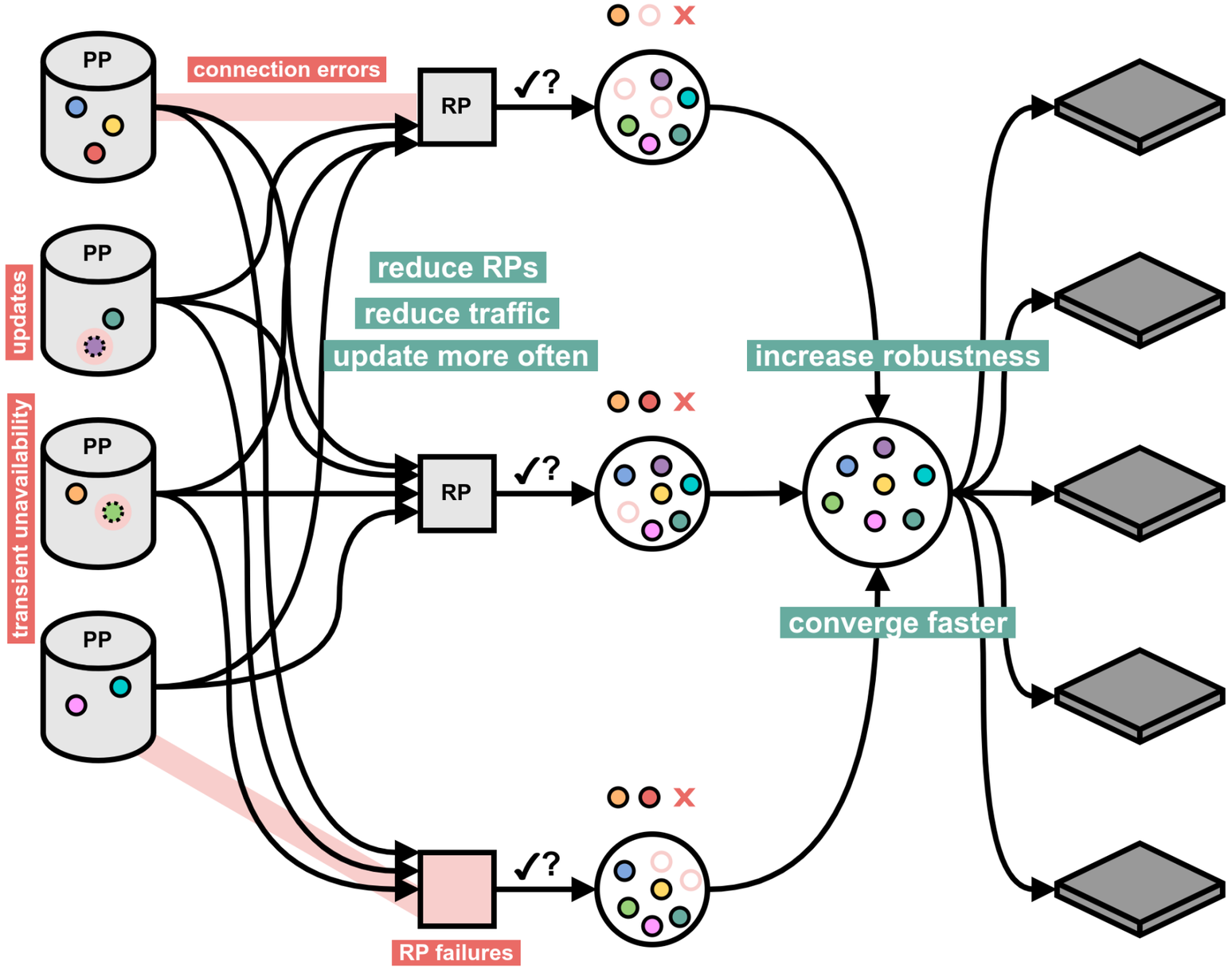
Inconsistent Object Sets Due to Instabilities



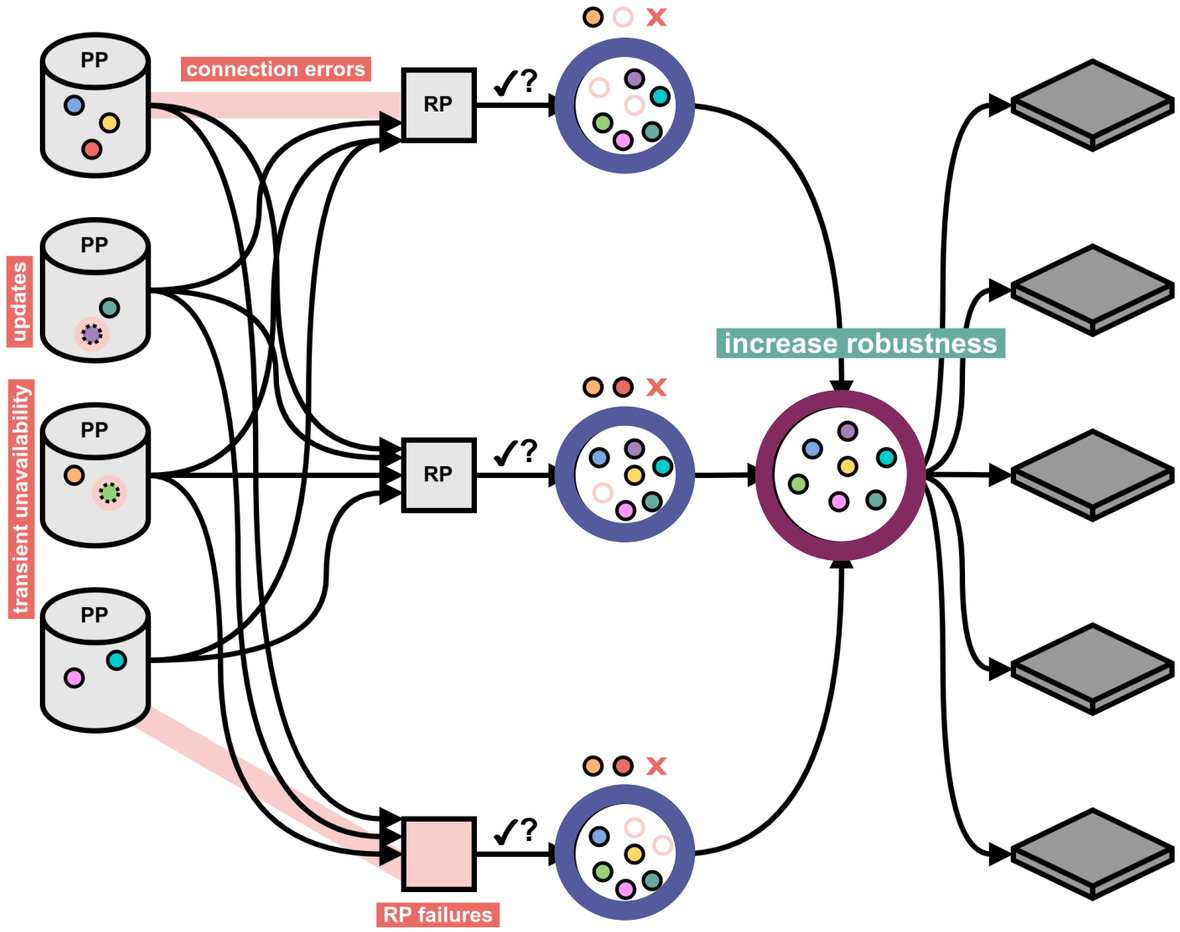
ByzRP: Robust Global Consensus

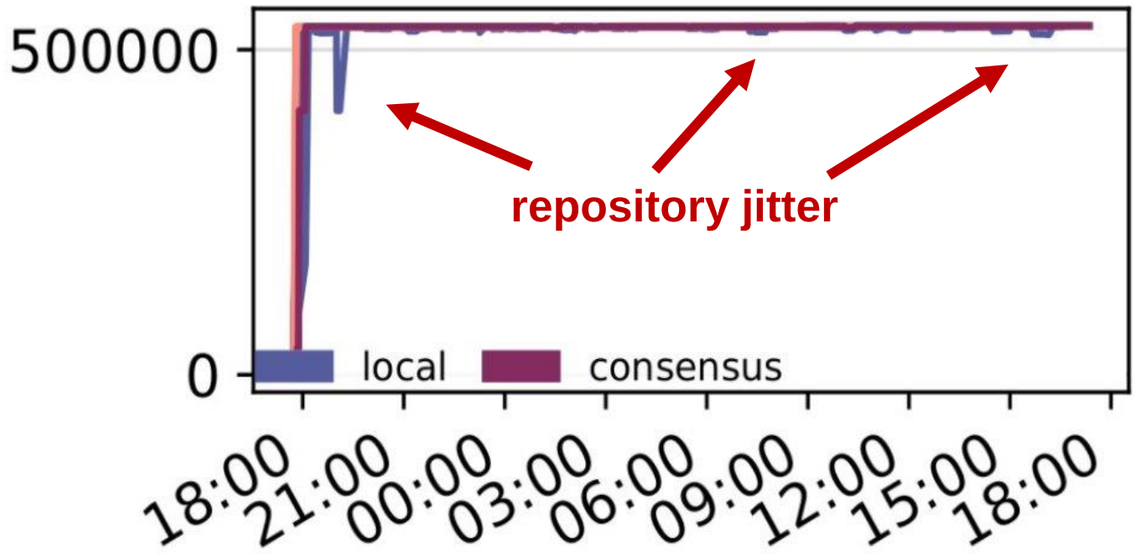


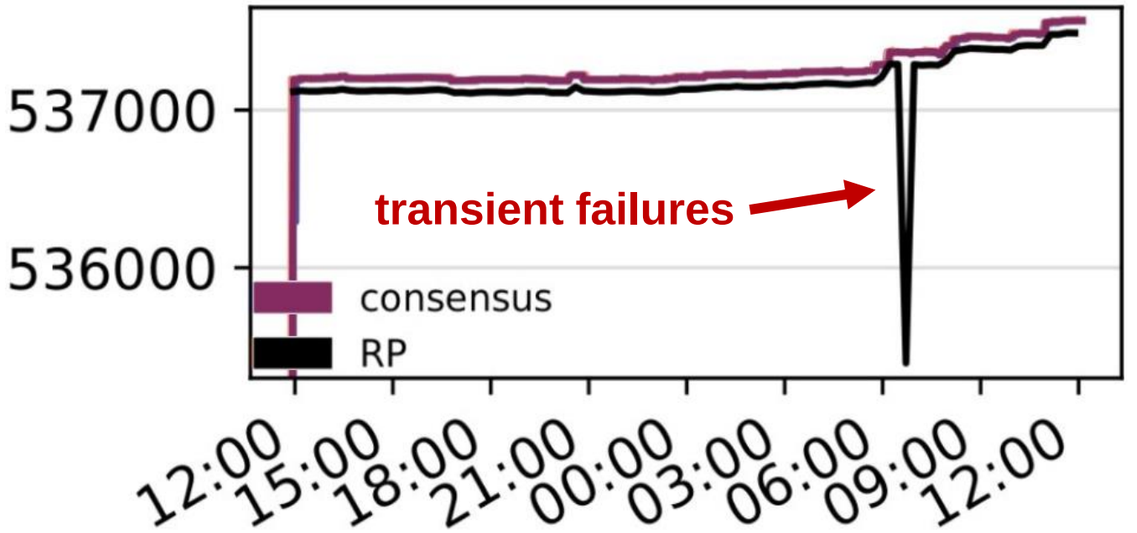
ByzRP: Robust Global Consensus



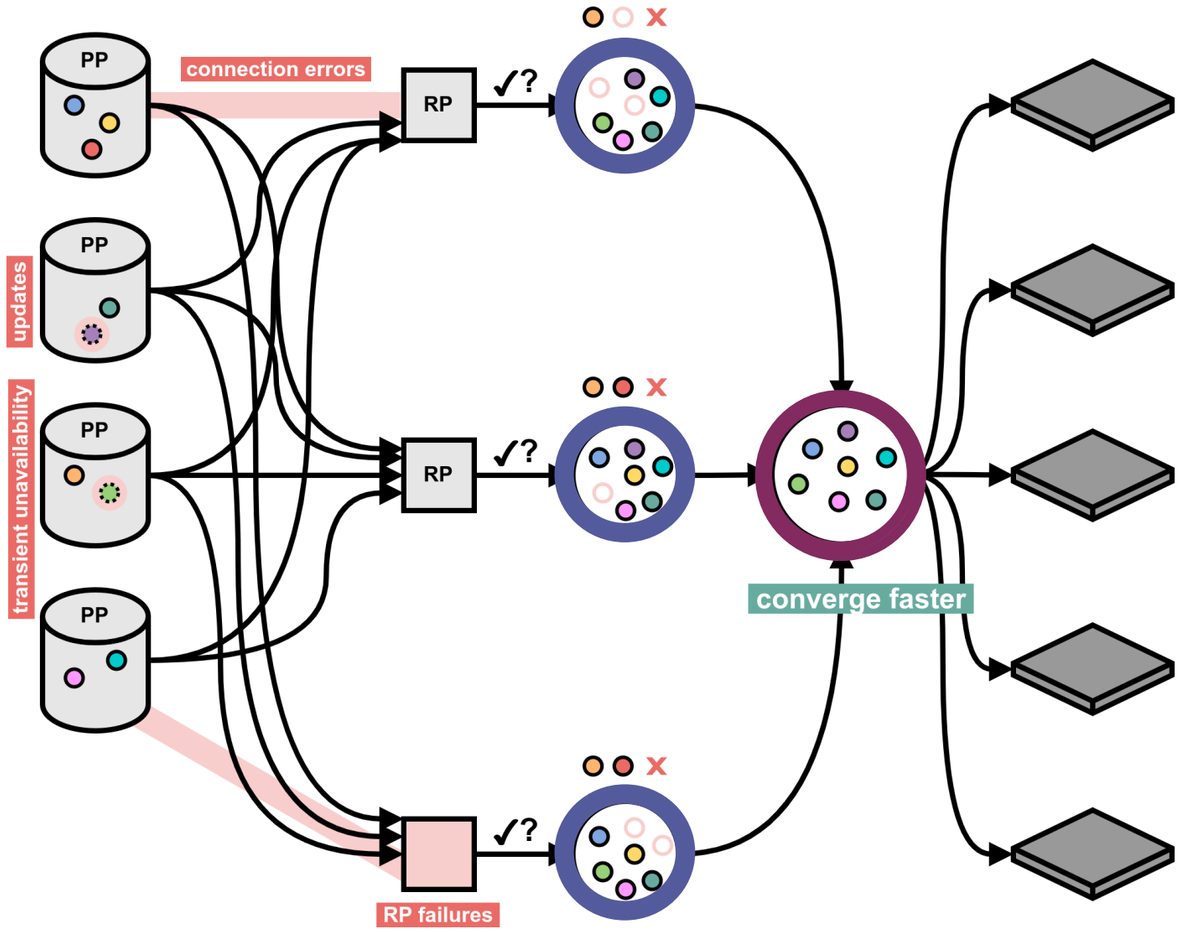
ByzRP: Jitter & Failure Resistant Output

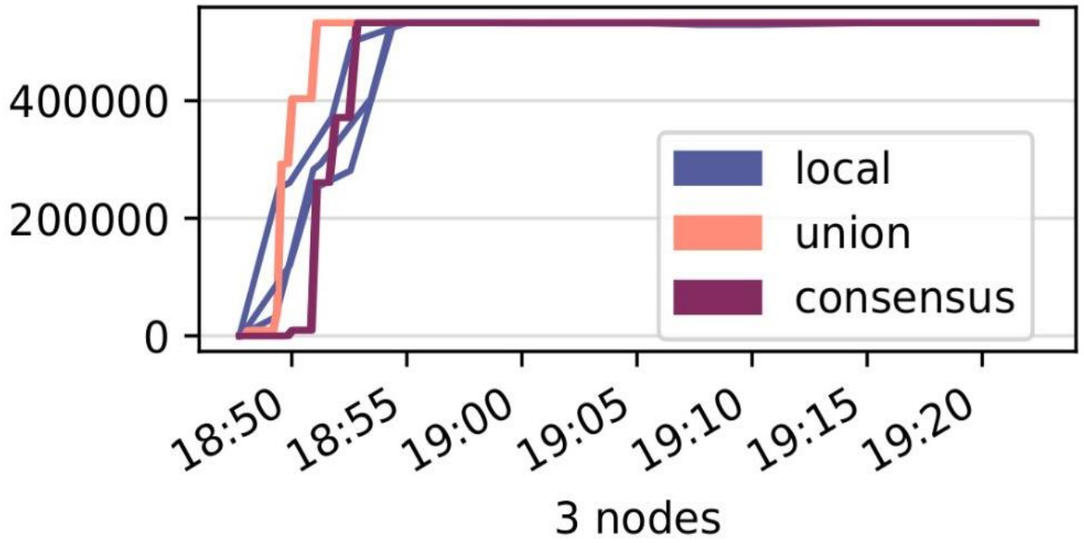


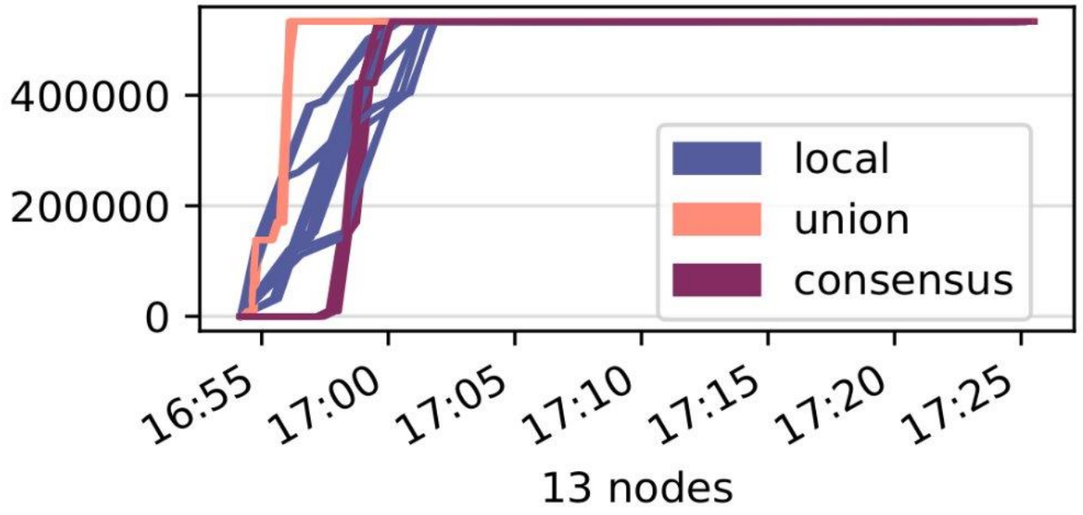




ByzRP: Fast Consensus Aggregation







should **everyone** run a ByzRP network?

should **everyone** run a ByzRP network?

not really...

ByzRP: RP-as-a-Service

should **everyone** run a ByzRP network?

not really...

better: a handful of operators run ByzRP nodes in a **global RP-as-a-Service** network

ByzRP: RP-as-a-Service

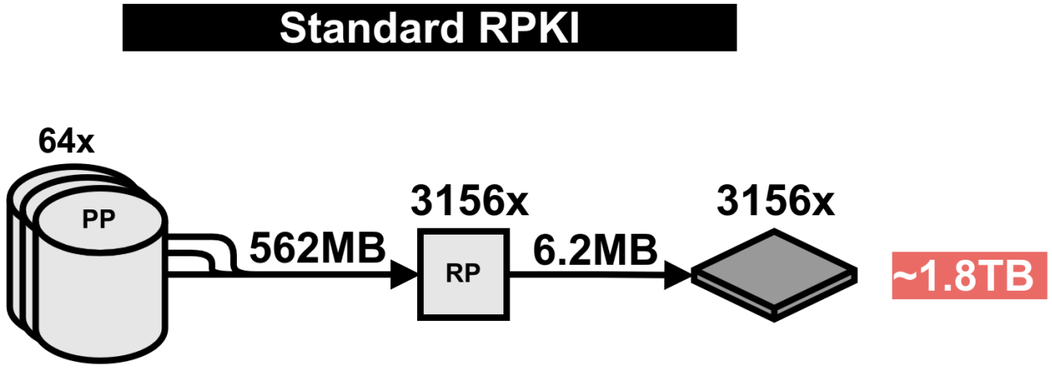
should **everyone** run a ByzRP network?

not really...

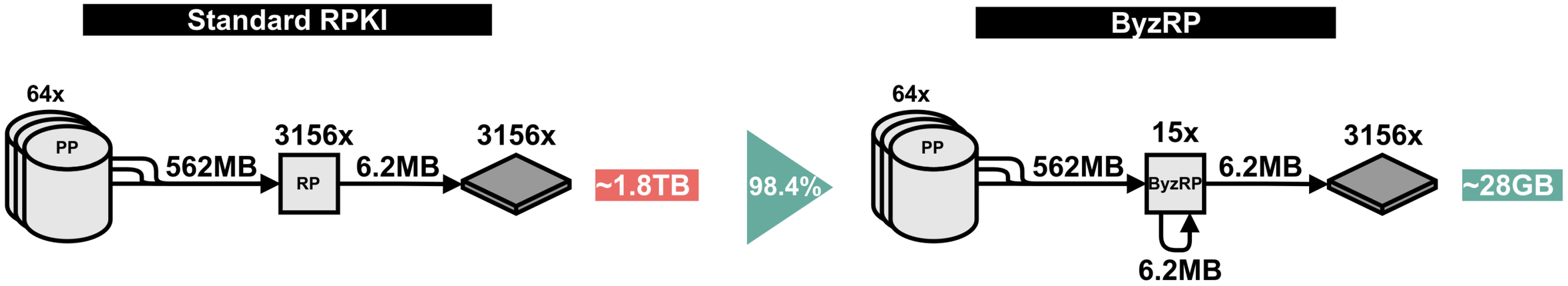
better: a handful of operators run ByzRP nodes in a **global RP-as-a-Service** network

1. not everyone needs to run their own RP
2. **reduced traffic** to PPs
3. allows more frequent updates

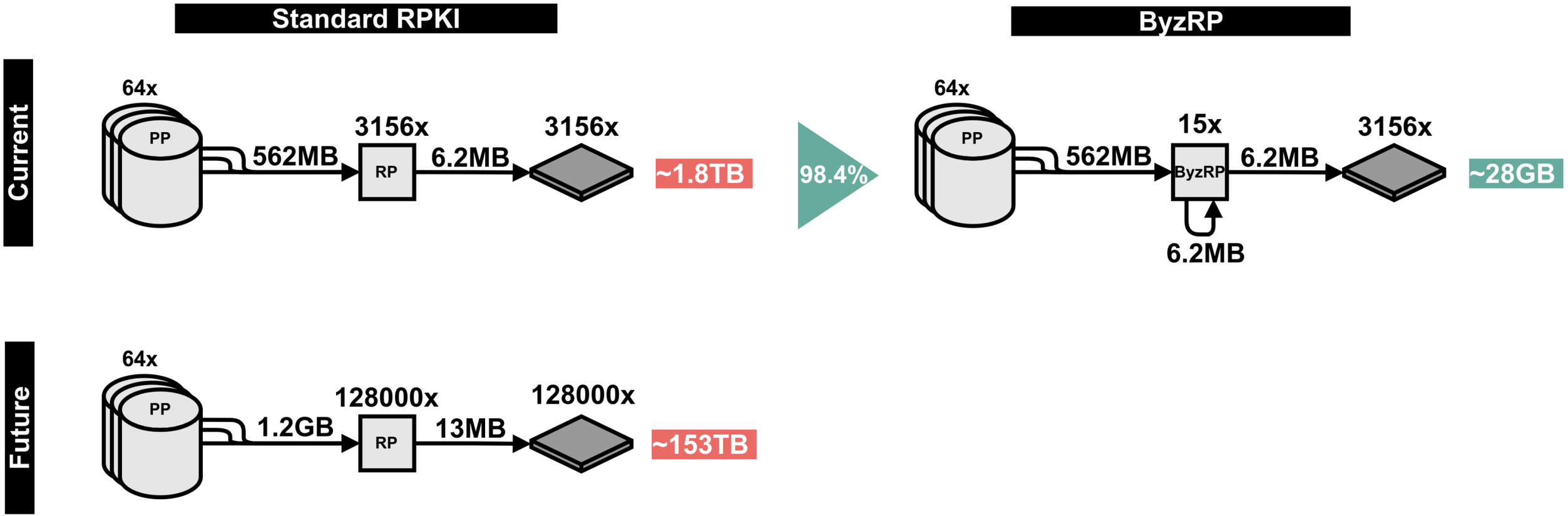
ByzRP: Traffic Reduction Through RP-as-a-Service



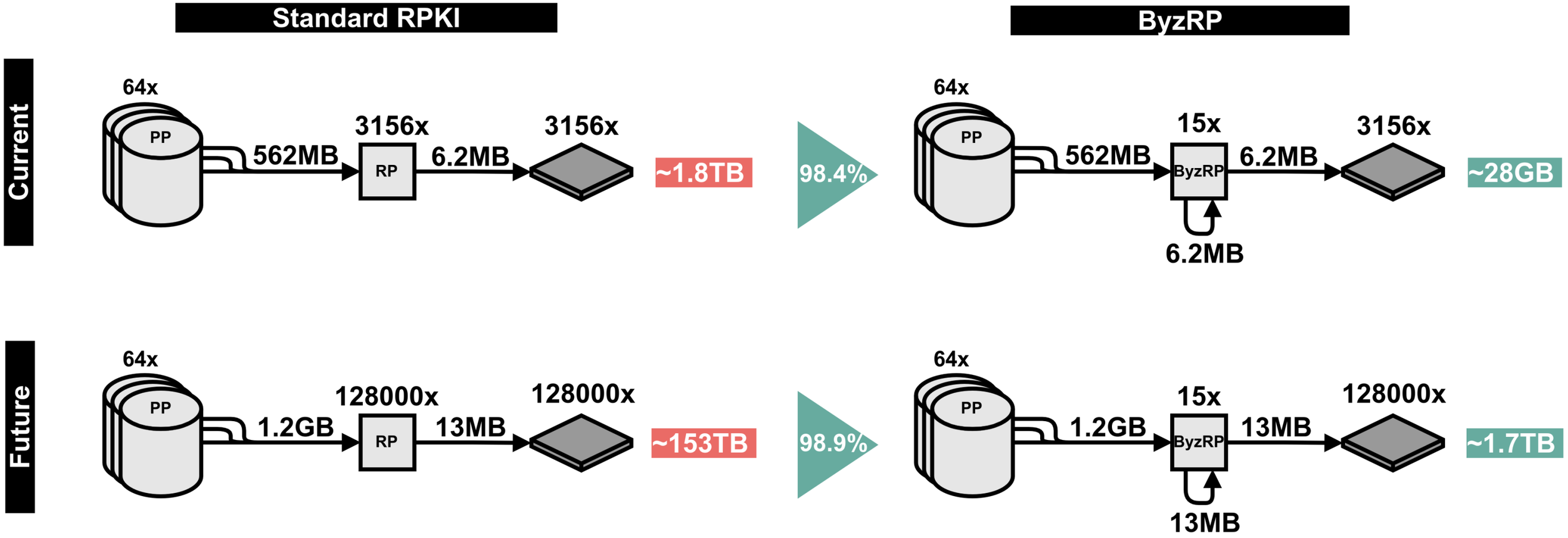
ByzRP: Traffic Reduction Through RP-as-a-Service



ByzRP: Traffic Reduction Through RP-as-a-Service



ByzRP: Traffic Reduction Through RP-as-a-Service



but RPs are **security-critical**!

but RPs are **security-critical**!

how can we trust **RPaaS**?

but RPs are **security-critical**!

how can we trust **RPaaS**?

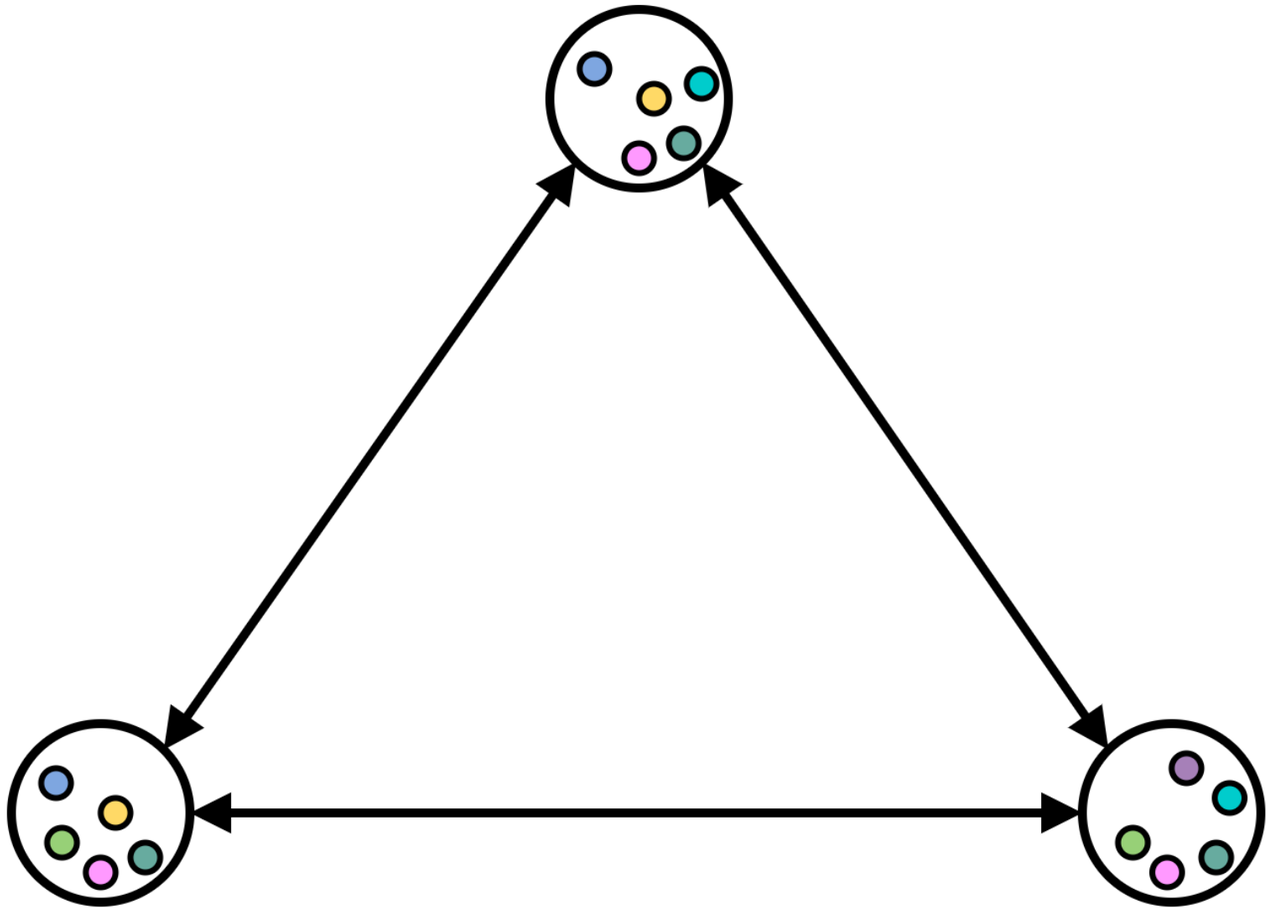
1. **distribute** nodes across distinct entities
2. trust in the **majority**

Consensus
With Byzantine Fault Tolerance

ByzRP: Consensus

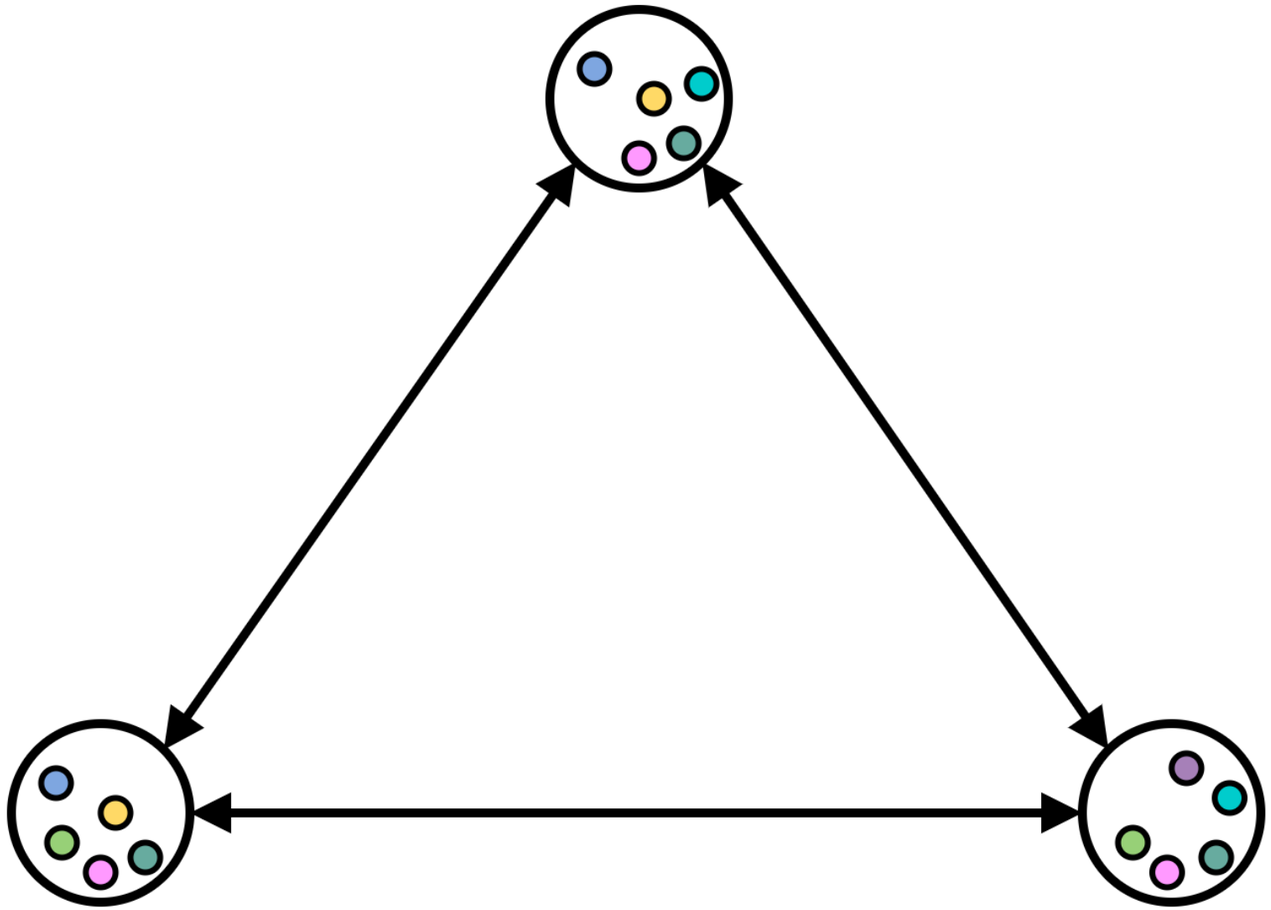
***N*=3** nodes

ByzRP: Consensus



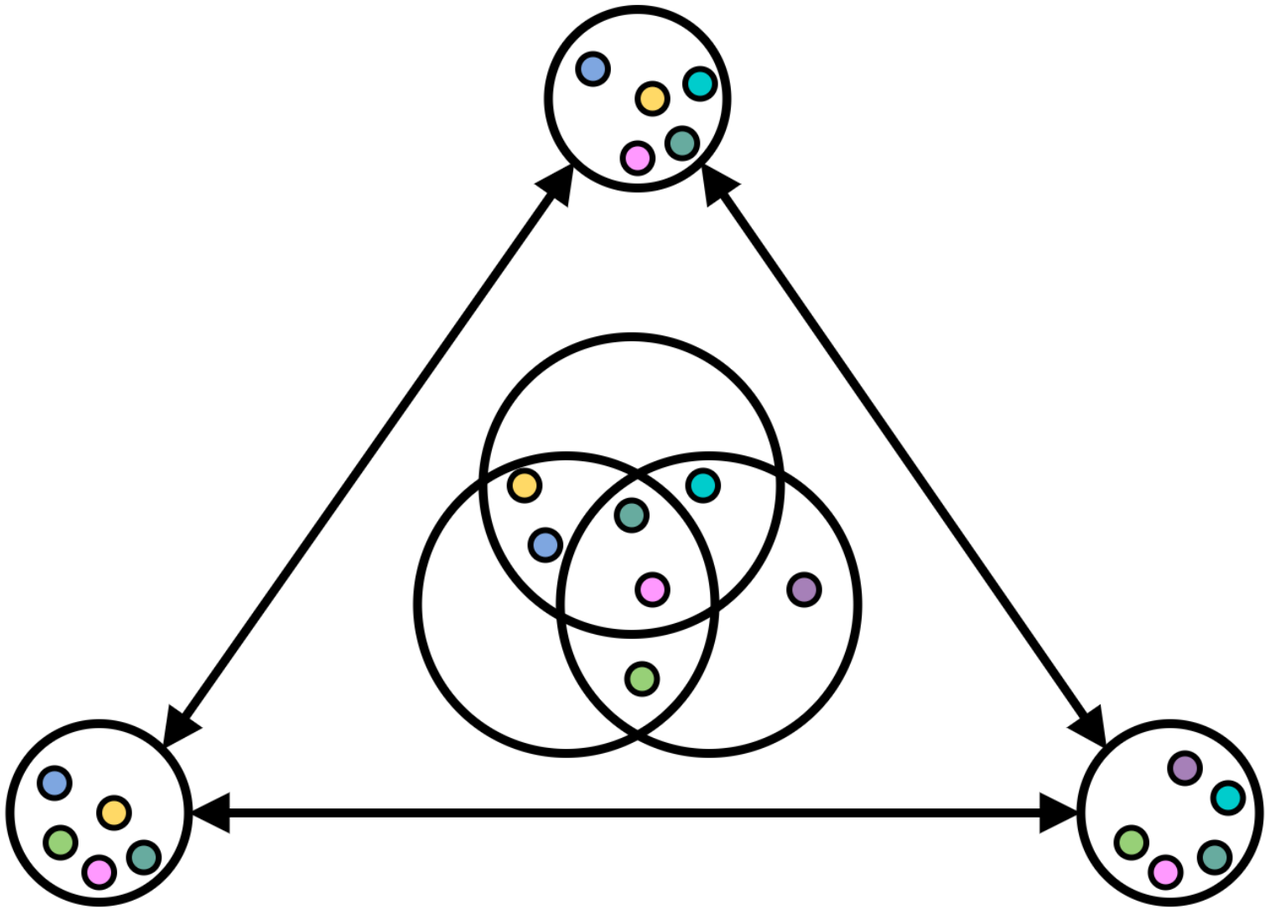
Fully-connected **permissioned** network through **mutual TLS**

ByzRP: Consensus



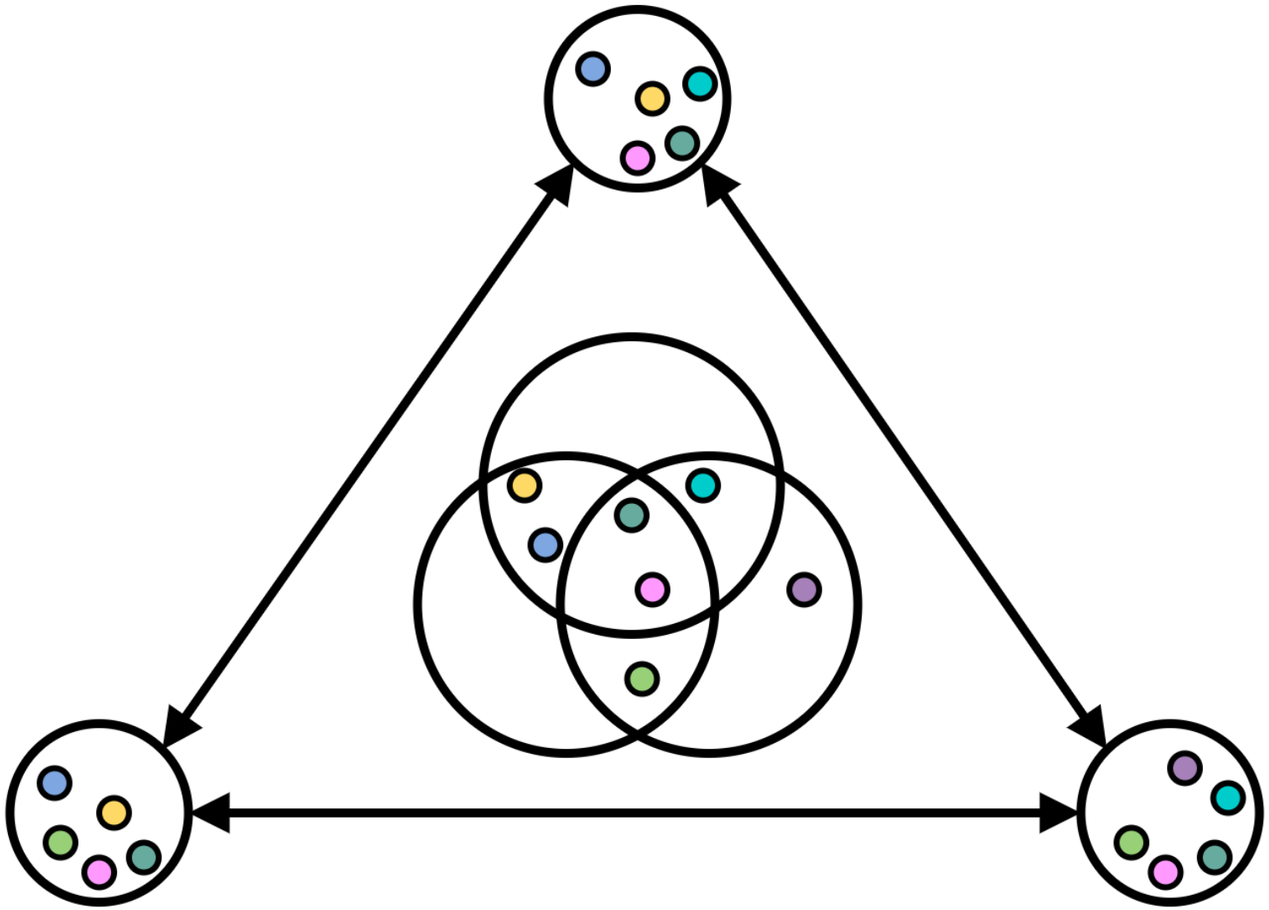
Each node **asynchronously polls**
its peers for their current object set

ByzRP: Consensus



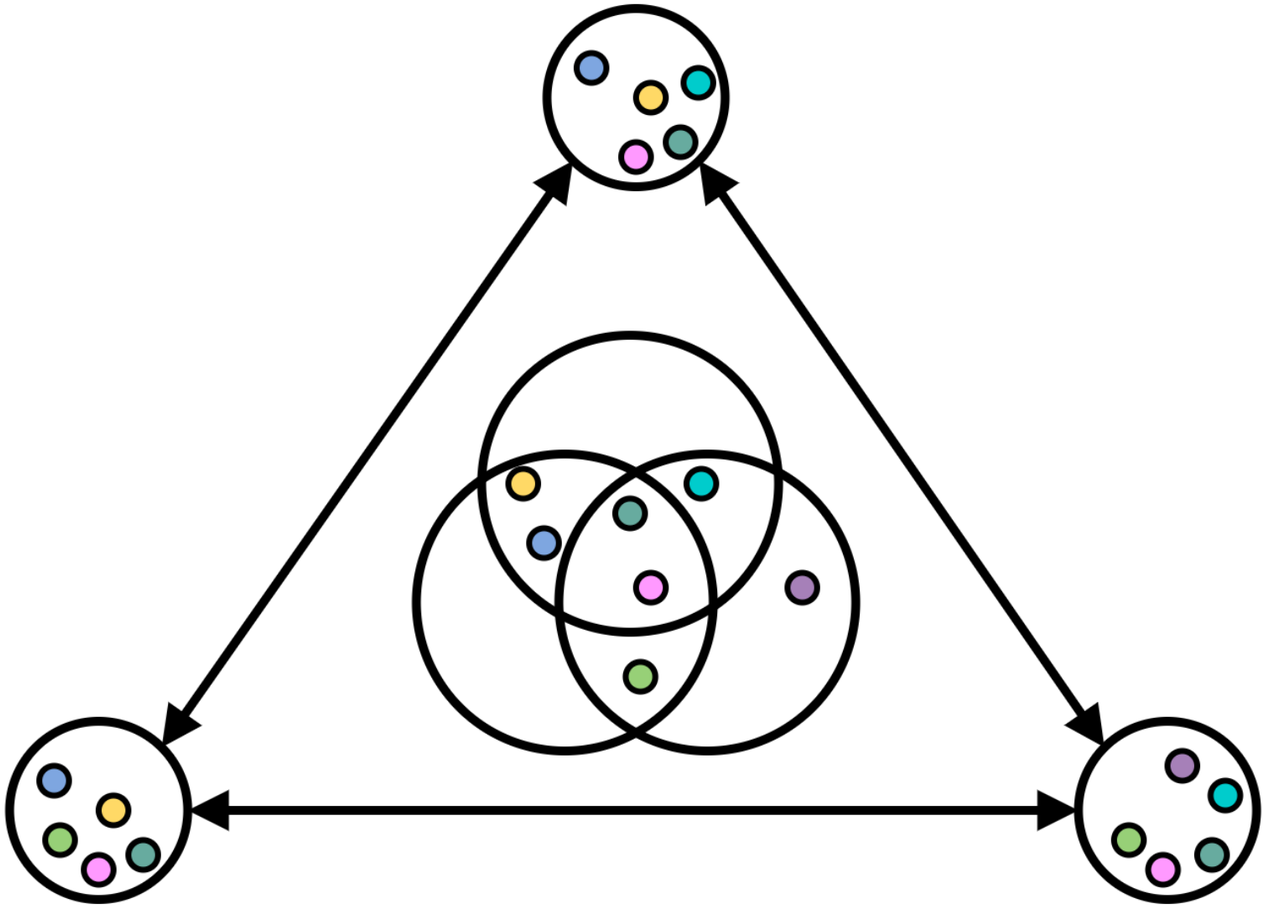
Each node can **independently** produce
the **same, deterministic** output
by intersecting object sets

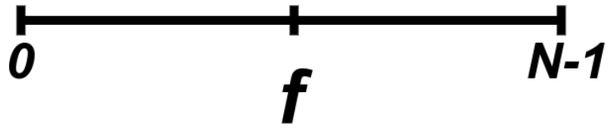
ByzRP: Consensus



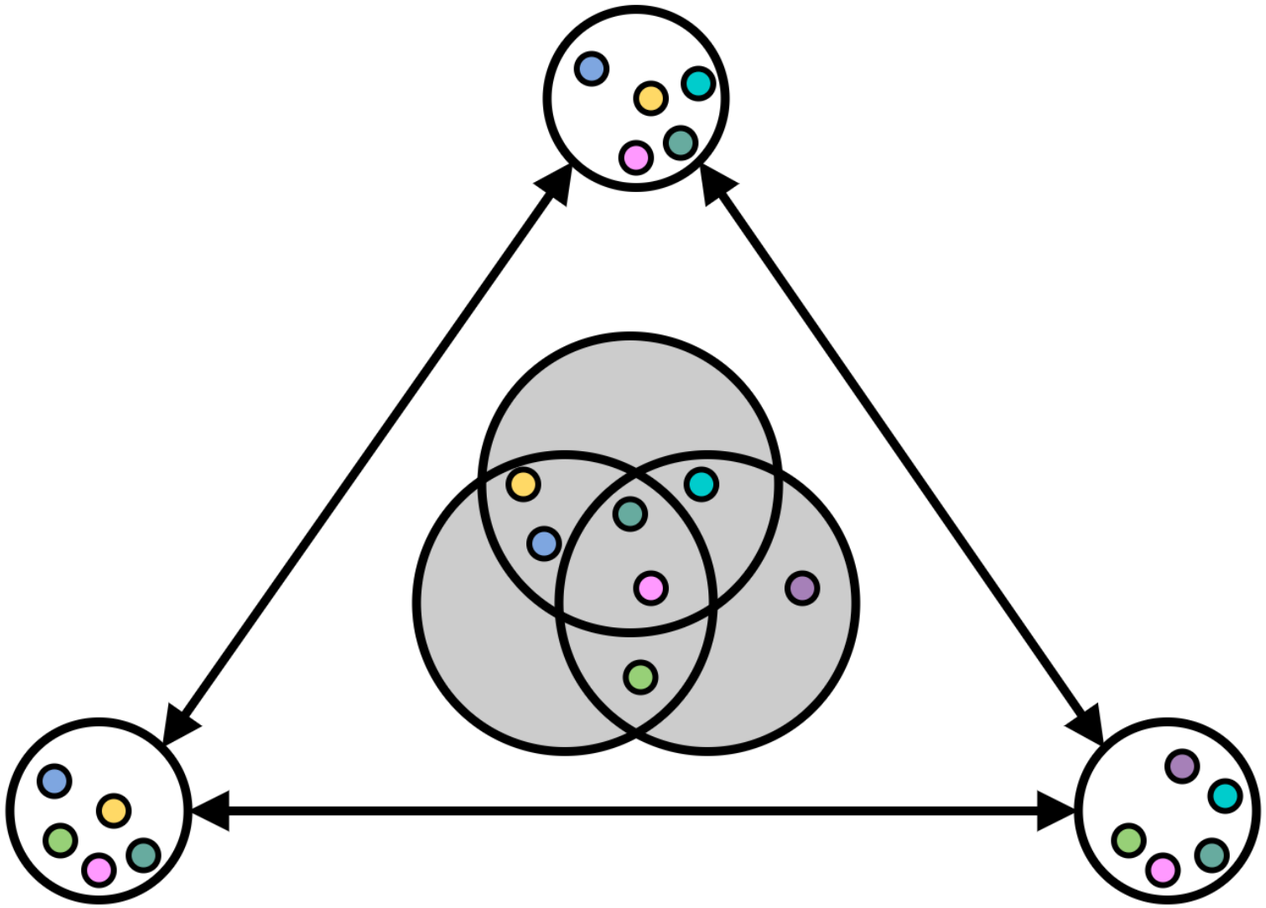
Secure against ***f*** **byzantine faults**
based on voting threshold

ByzRP: Consensus



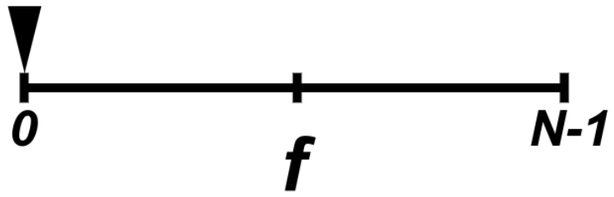


ByzRP: Consensus

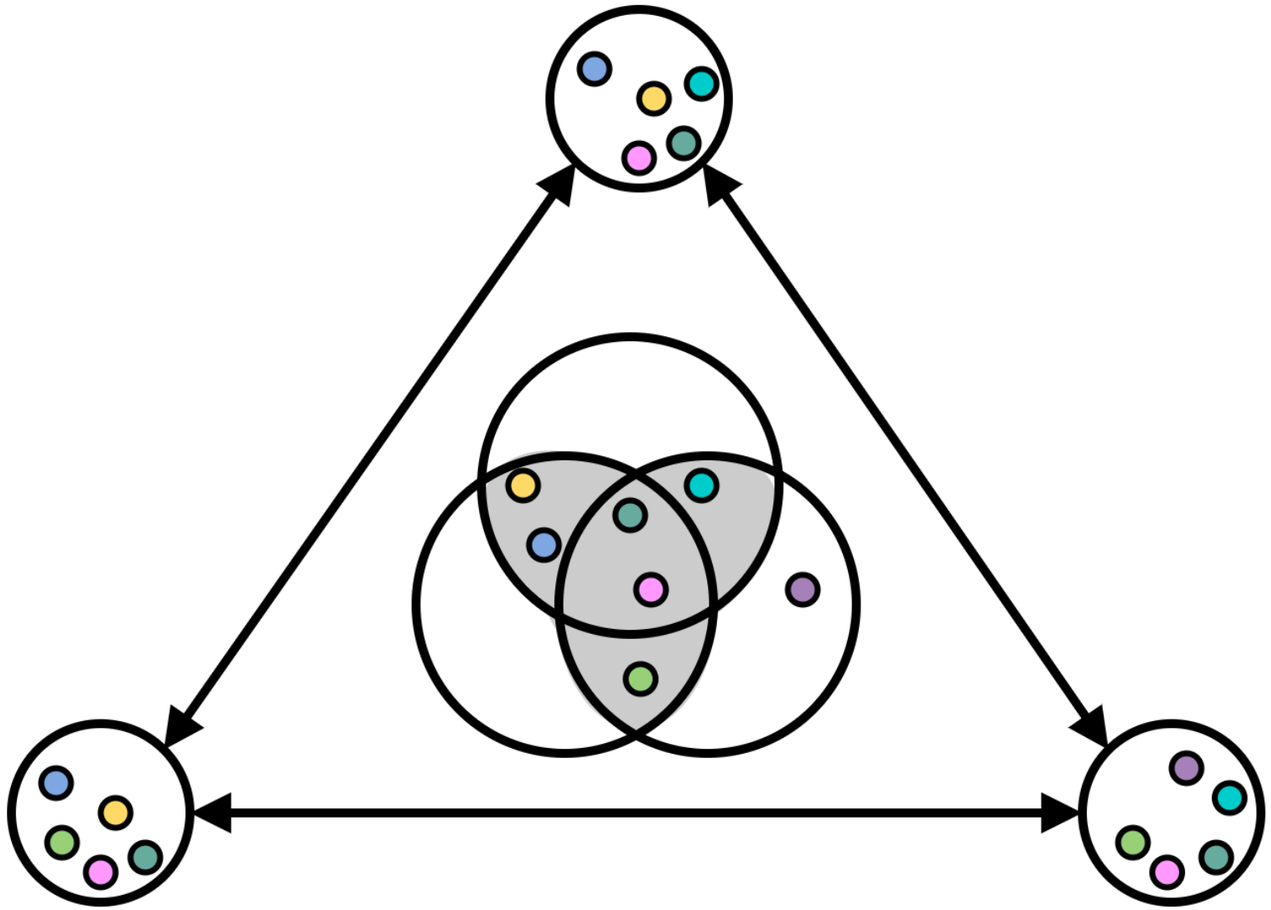


1-out-of-3 = union

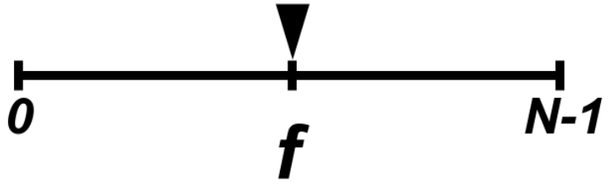
resist **censorship / errors**



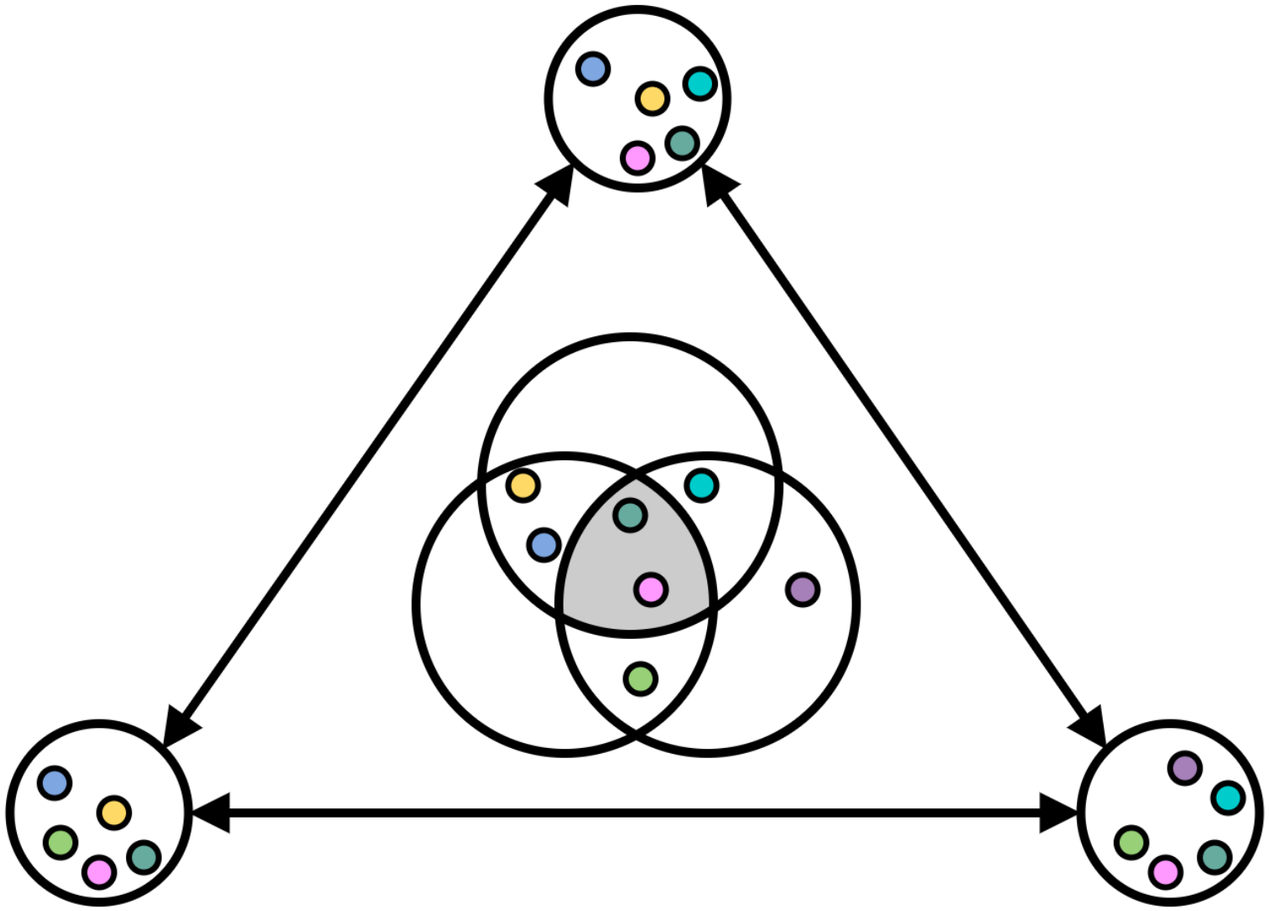
ByzRP: Consensus



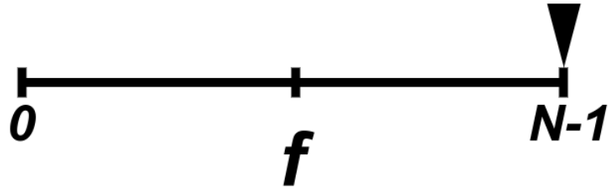
2-out-of-3 = majority



ByzRP: Consensus

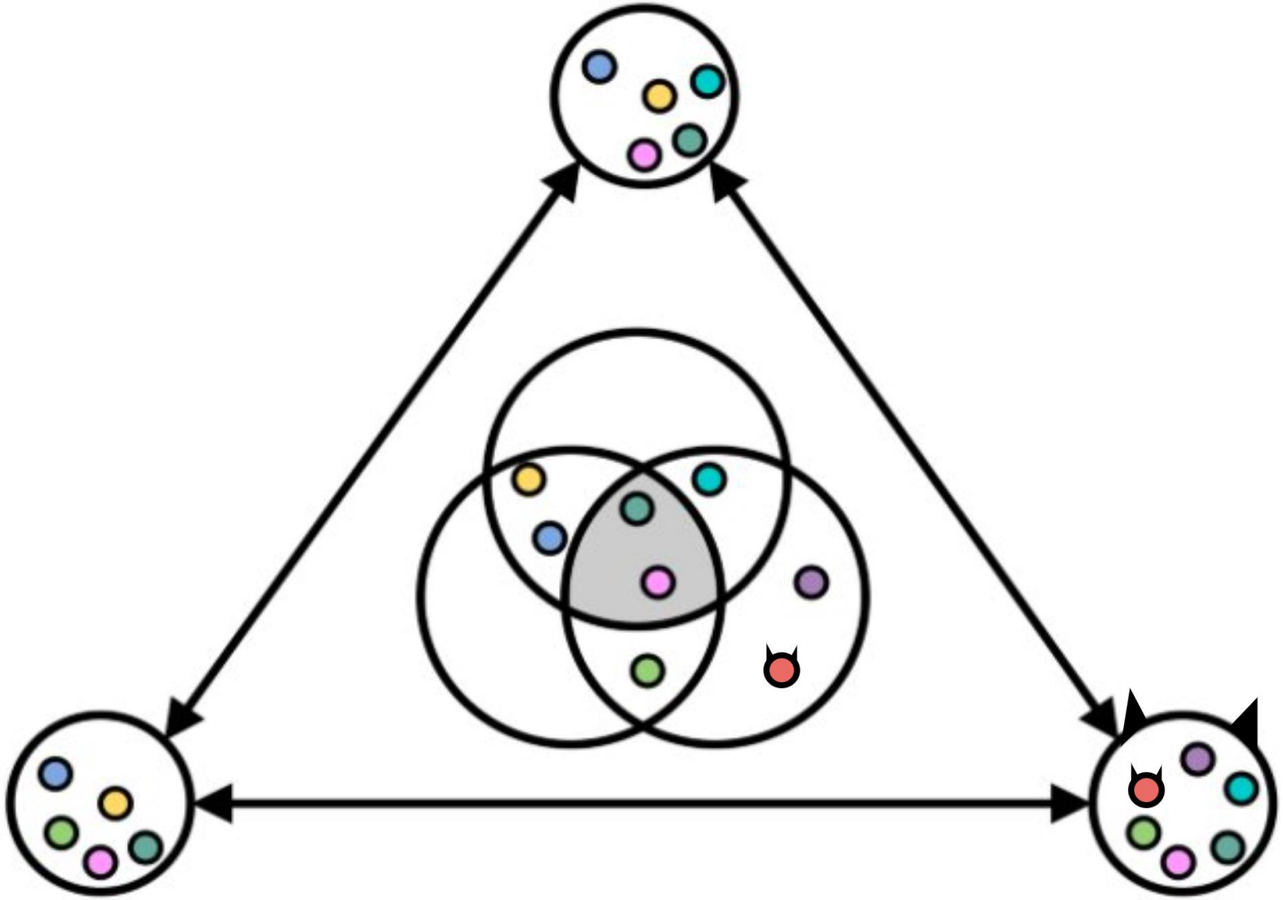


3-out-of-3 = unanimity = intersection

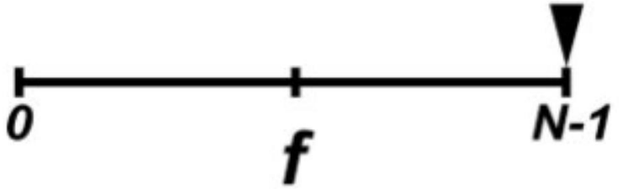


resist **poisoning**

ByzRP: Consensus Poisoning

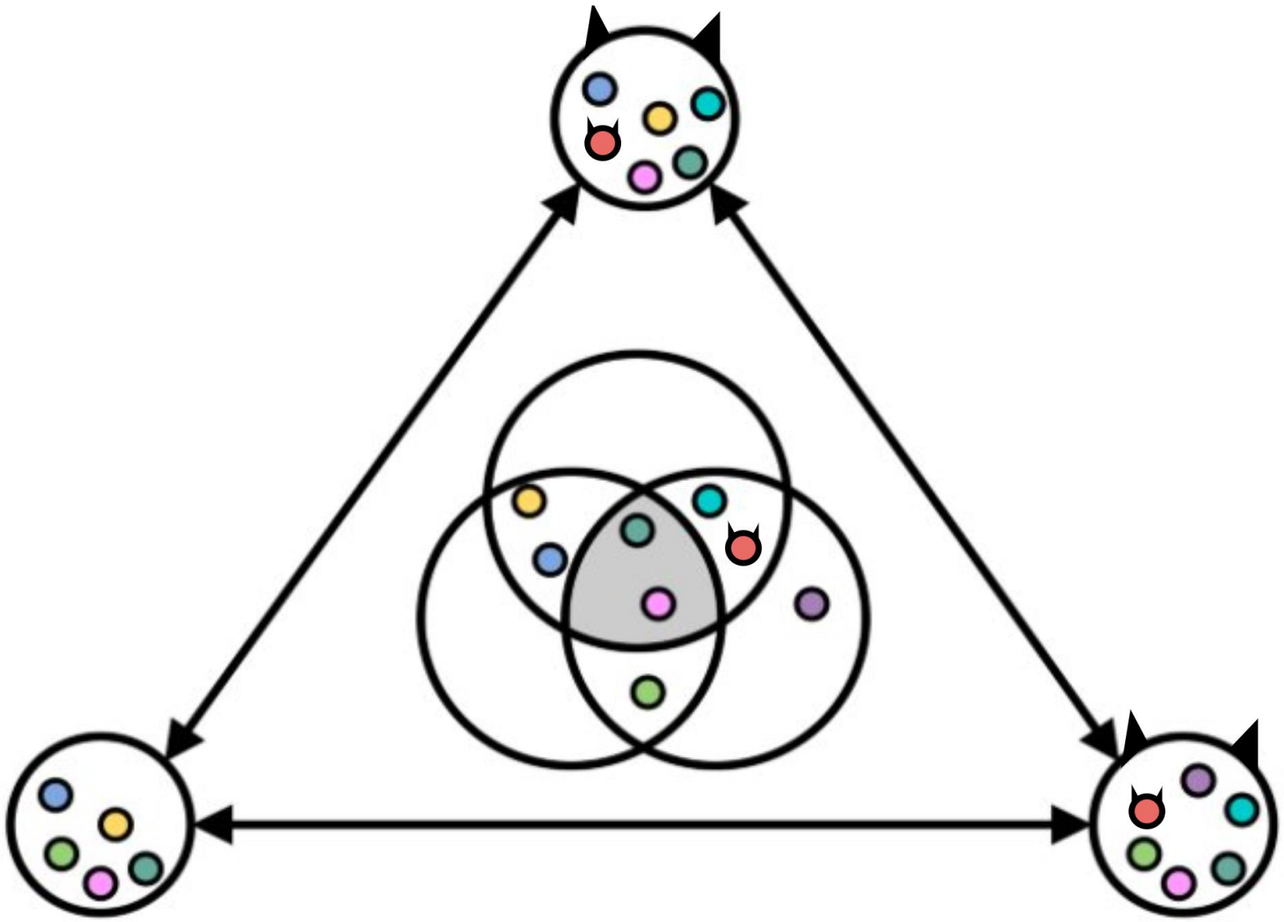


3-out-of-3 = unanimity = intersection

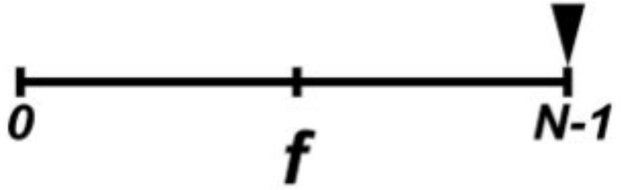


resist **poisoning**

ByzRP: Consensus Poisoning

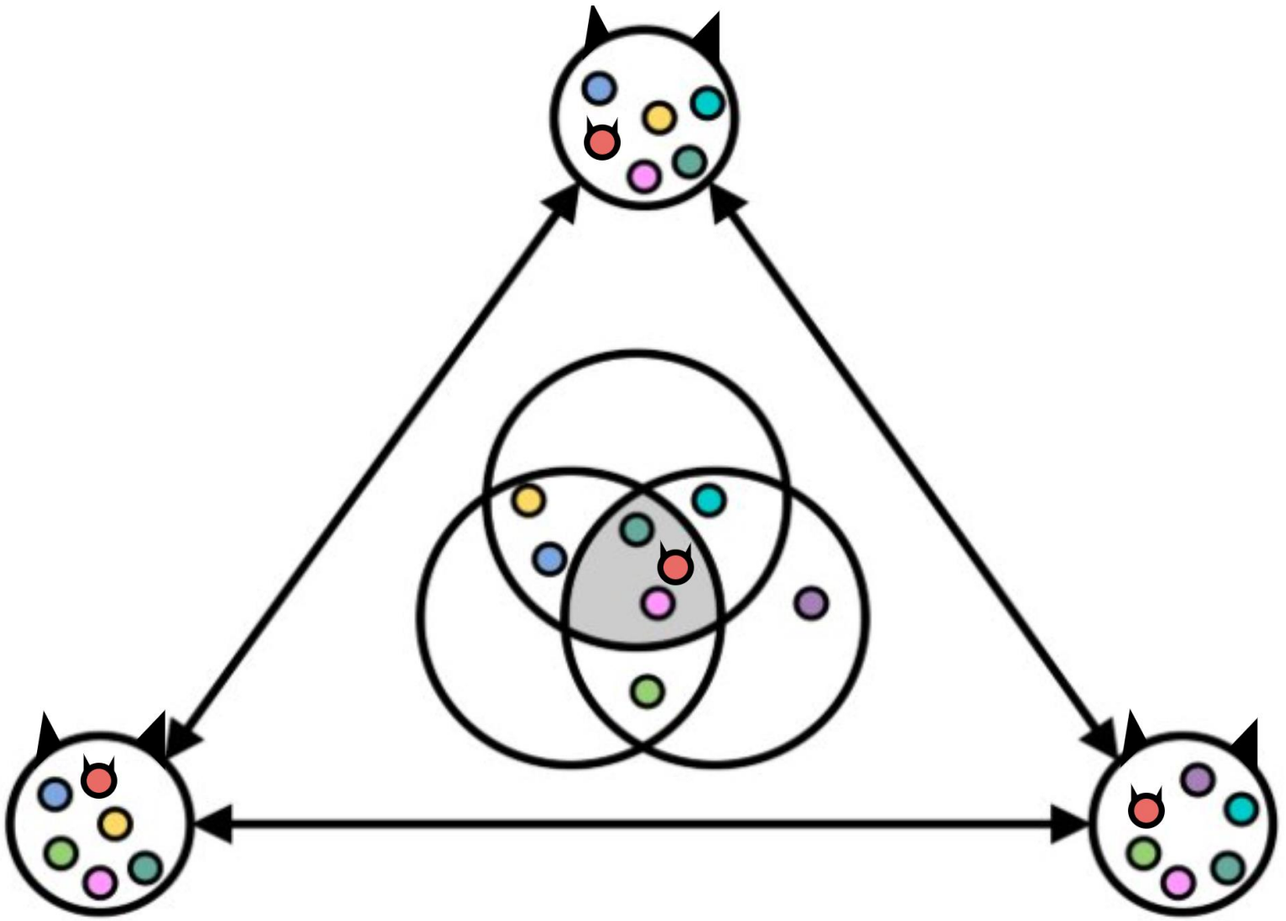


3-out-of-3 = unanimity = intersection

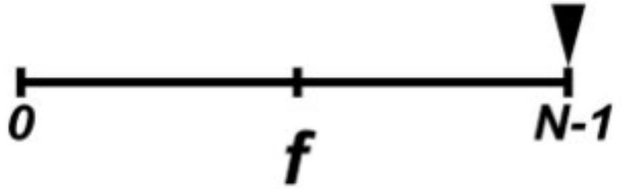


resist **poisoning**

ByzRP: Consensus Poisoning

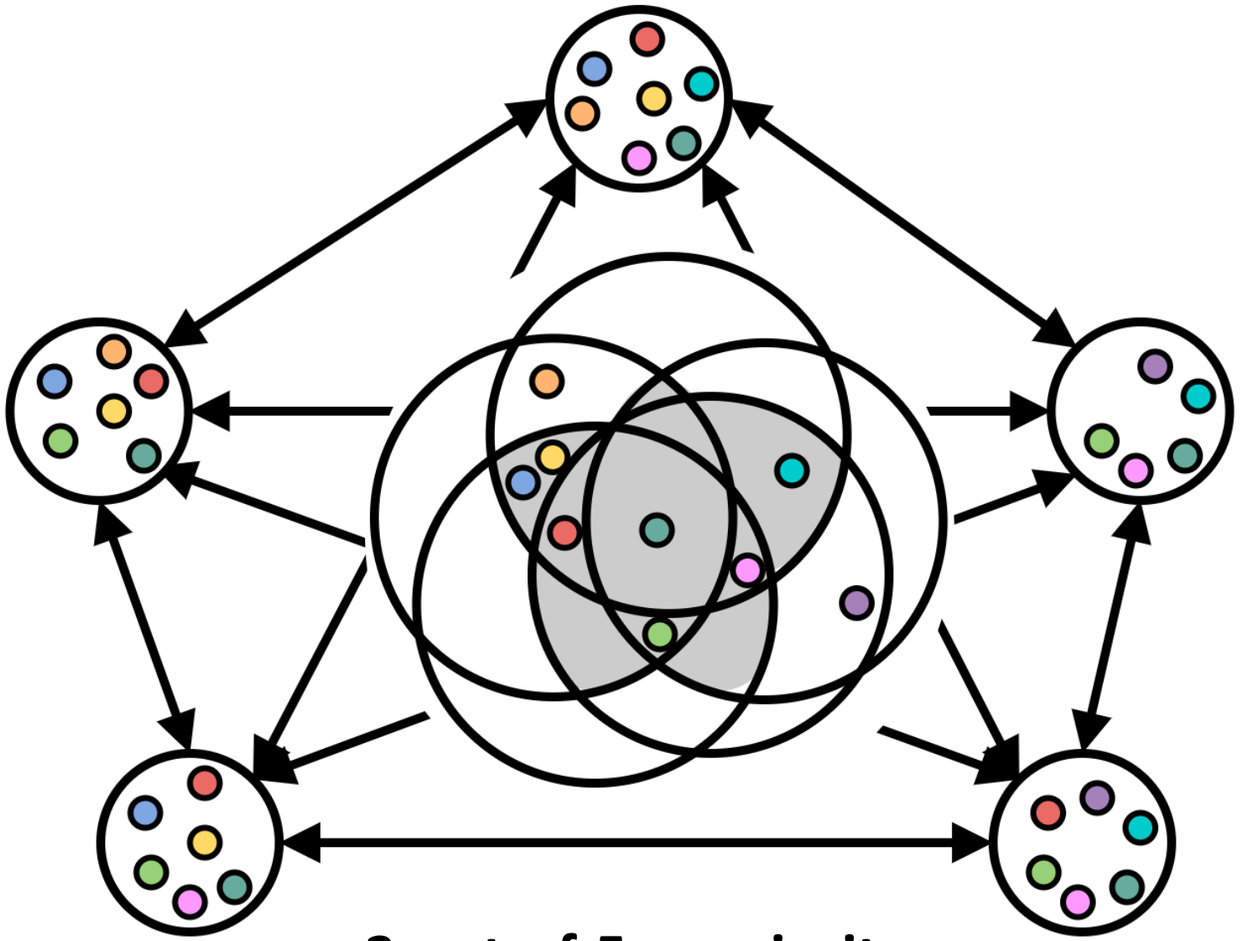


3-out-of-3 = unanimity = intersection



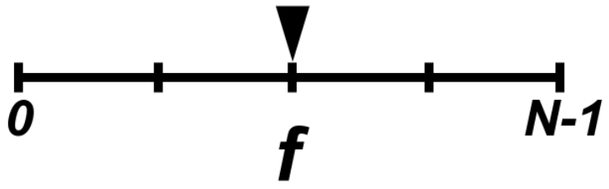
resist **poisoning**

ByzRP: Consensus



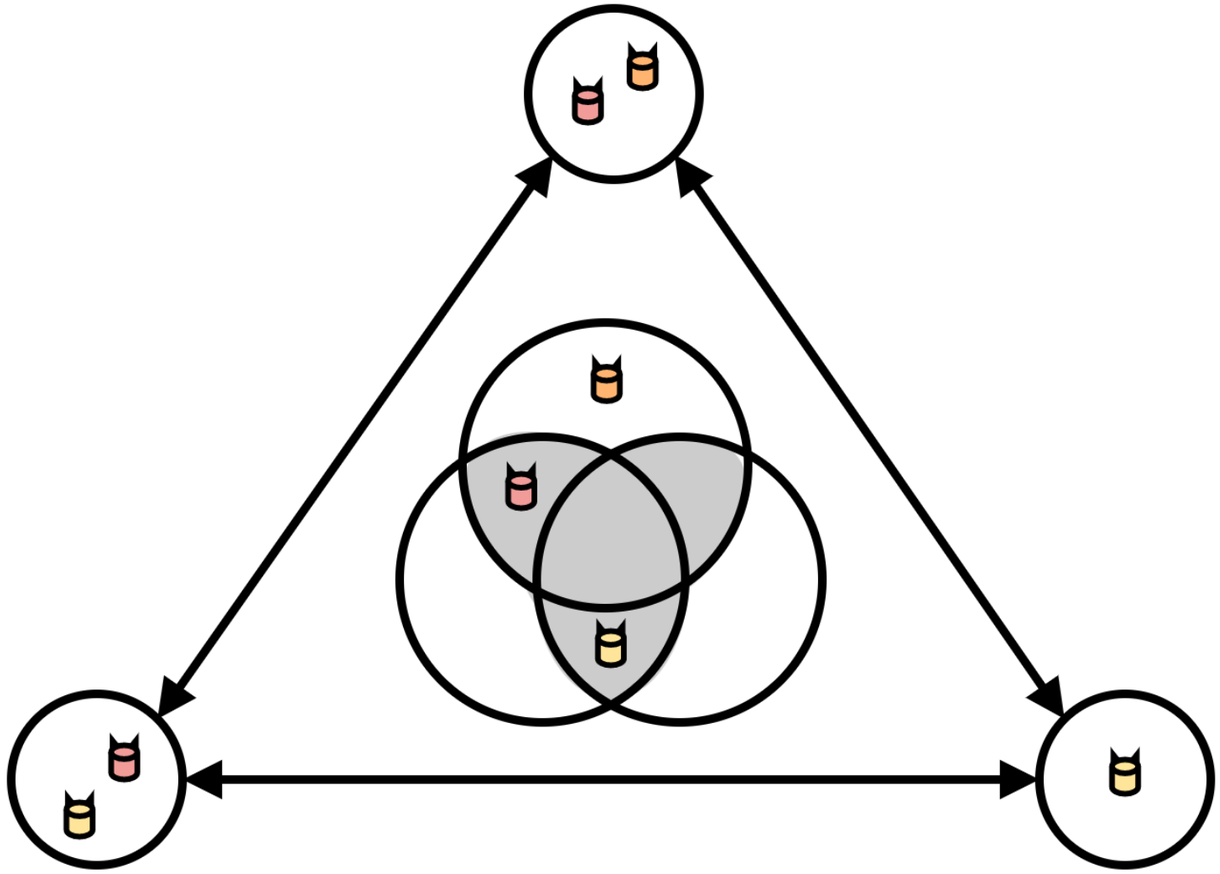
3-out-of-5 = majority

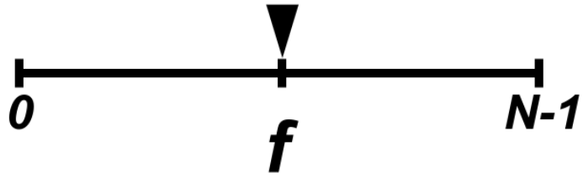
faster **inclusion**



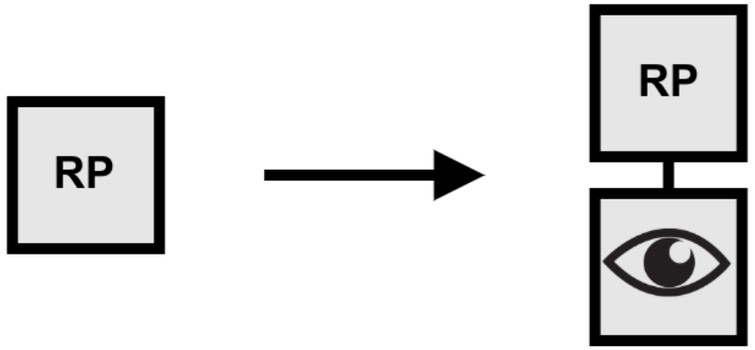
faster **removal**

ByzRP: Consensus for Watchdog Skiplist Entries



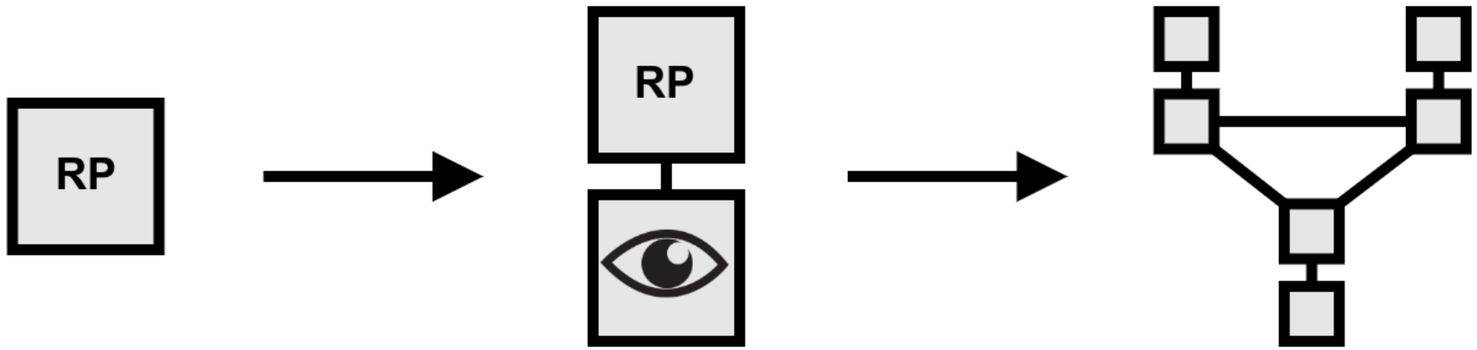


Summary



- stalling protection
- crashing protection
- adaptive skiplisting

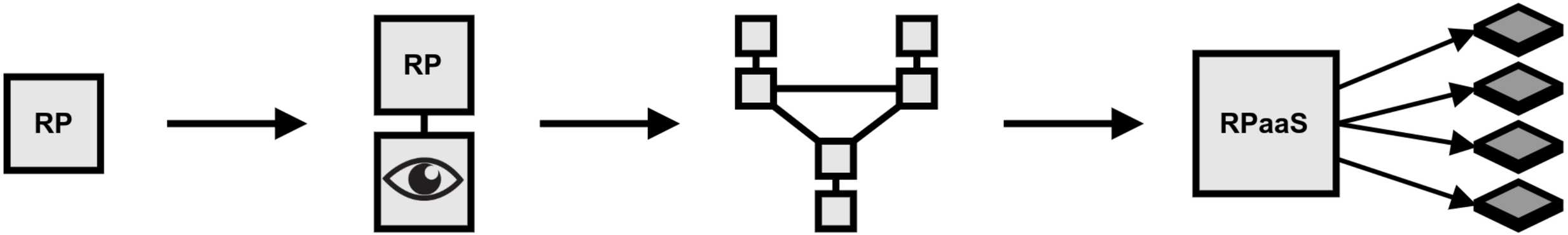
Summary



- stalling protection
- crashing protection
- adaptive skiplisting

- parallel processing
- asynchronous consensus
- byzantine fault tolerance
- distribution of trust

Summary

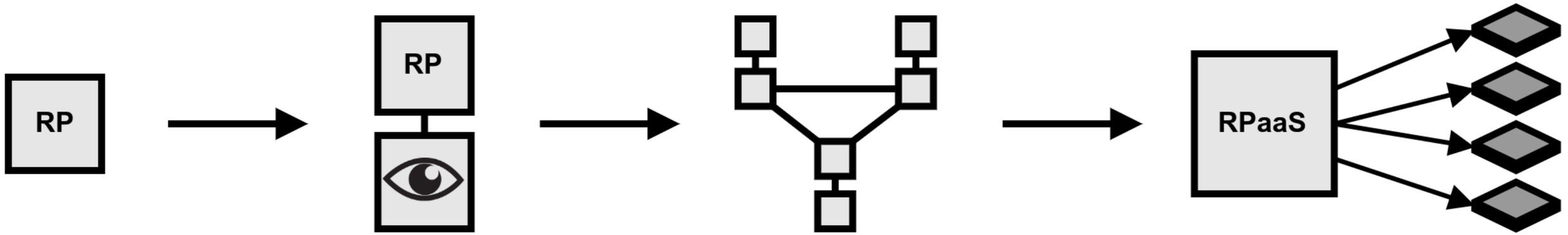


- stalling protection
- crashing protection
- adaptive skiplisting

- parallel processing
- asynchronous consensus
- byzantine fault tolerance
- distribution of trust

- reduced network traffic
- higher update frequency
- easier RPKI adoption

Summary



- stalling protection
- crashing protection
- adaptive skiplisting

- parallel processing
- asynchronous consensus
- byzantine fault tolerance
- distribution of trust

- reduced network traffic
- higher update frequency
- easier RPKI adoption

MORE **ROBUSTNESS**

MORE **PERFORMANCE**

MORE **RPKI ADOPTION**

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

jens.friess@athene-center.de

donika.mirdita@athene-center.de

github.com/Cyberbruecke/byzrp

acm SIGSAC

doi/pdf/10.1145/3658644.3690368