

DS 593: Privacy in Practice

Blockchains Continued and Federation

News?



NATIONAL
BEAGLE
DAY THURSDAY,
APRIL 22



Last time

- Consensus and Blockchains

Today

- Wrapping up Blockchains
- Federation

Blockchains

- A system for coming to distributed/decentralized consensus
- Formally introduced in the Bitcoin whitepaper
 - Builds on earlier ideas by Chaum, Haber, Bayer, Stornetta
 - Byzantine Fault Tolerance



Bitcoin

- A cryptocurrency proposed by Satoshi Nakamoto in 2009
 - Who?
- A cryptocurrency is a decentralized payment system, generally built on top of a blockchain
 - Bitcoin was first prominent example, but ecash dates back to 1983
- Blockchains and cryptocurrencies have a bit of a symbiotic relationship

The Bitcoin Protocol

- Uses a proof-of-work based blockchain
- Peers run the bitcoin client which manages interaction with the rest of the network
 - Official vs Unofficial Clients
- A P2P payment system

Bitcoin Mining

- Miners are the peers competing to generate the next block
- The goal was 1 person 1 vote
- Miners are incentivized as having your block accepted comes with some Bitcoin as a reward

Bitcoin Accounts and Transactions

- Your bitcoin account is represented by a public key pair
 - Each of your bitcoins is “signed”
 - Linked to the public key and possession of private key shows ownership
 - What happens if you lose your key?
- “Spending” a coin involves using your private key and the recipients public key
- You produce a transaction that is sent to the network



Bob
receives

TX A



Bob
spends

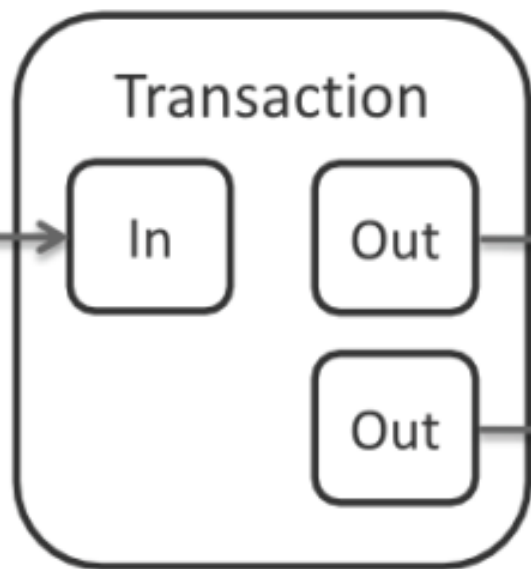


Alice
receives



Alice
spends

50 BTC
from an
investment



0.5 BTC
to **Alice**

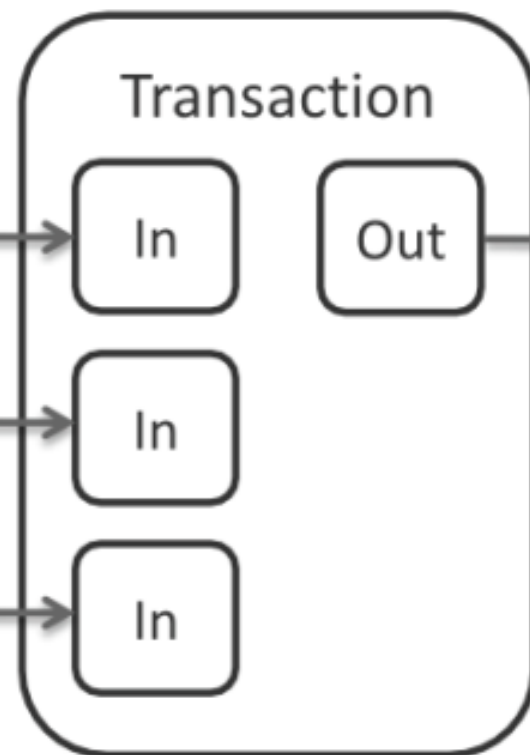
49.5 BTC
to his
change
address

TX B

0.5 BTC
from **Bob**

0.1 BTC
from a
stranger

0.2 BTC
from her
sister



0.8 BTC
to her
employee

Bitcoin transactions

- Peers, and in particular, miners see new transactions as they are broadcast to the network
- Miners include the transactions they see into the blocks they propose
 - They get a “fee” for including a transaction
- Once a block containing a transaction is confirmed by the network, it is officially considered spent
 - Why is this binding?

How to get Bitcoin

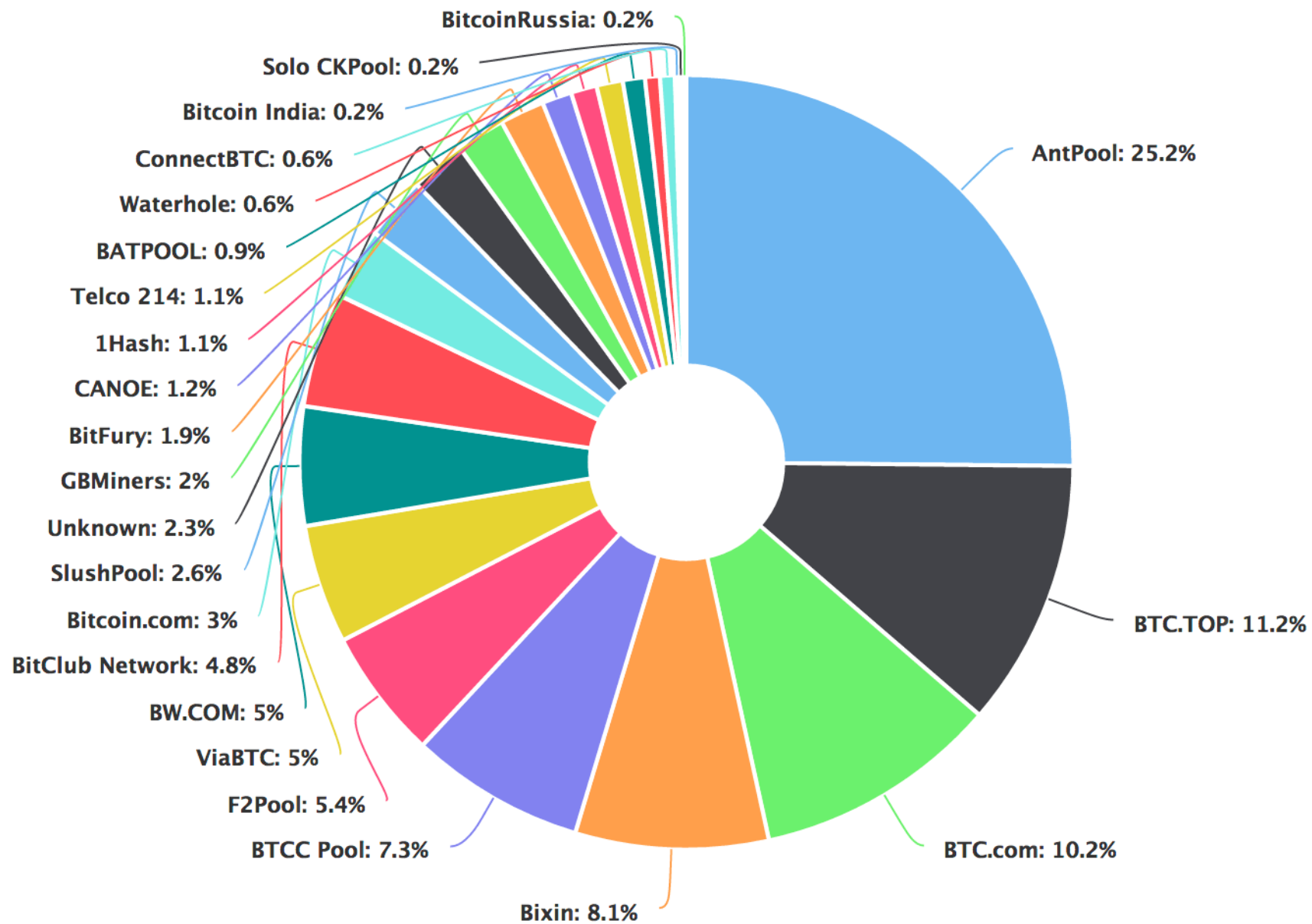
- Exchanges
- Mine a new block and get a reward
- Mine a new block and get fees

Challenges and considerations

- Not exactly "1 person 1 vote"
- Exchanges can lead to some centralization
- Fees can get quite high
- Hard to change
- Is it actually private?

Modern Mining





Coinbase website down as crypto exchange cites 'system-wide outage'

Crypto exchange Coinbase suffered a "system-wide" outage, rendering the platform unusable.

11125 Total views

5 Total shares

Listen to article

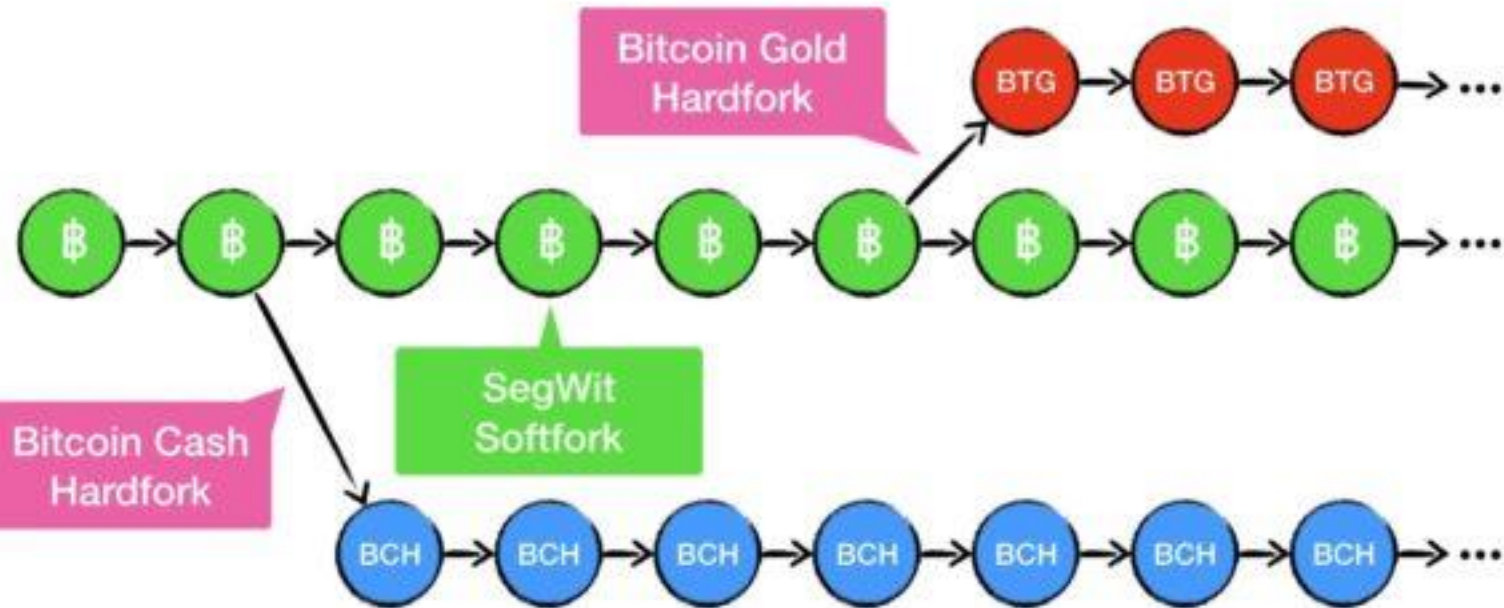


1:11





Bitcoin Forks 2017



Is Bitcoin private/anonymous

- Account is only linked to your key pair
 - More like a pseudonym
 - Often gets reused
- Transactions are only linked to this account as well

PRESS RELEASE

Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside



Monday, June 7, 2021

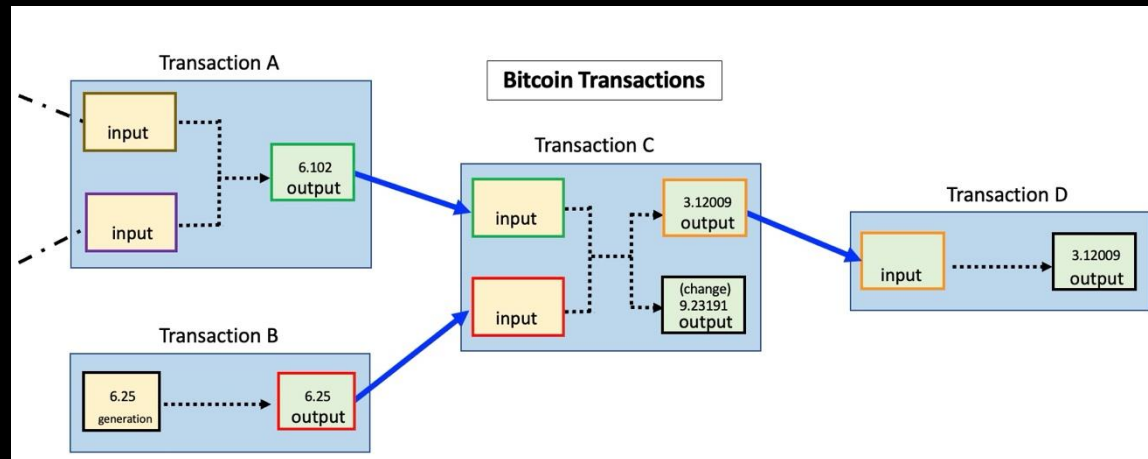
For Immediate Release

Office of Public Affairs

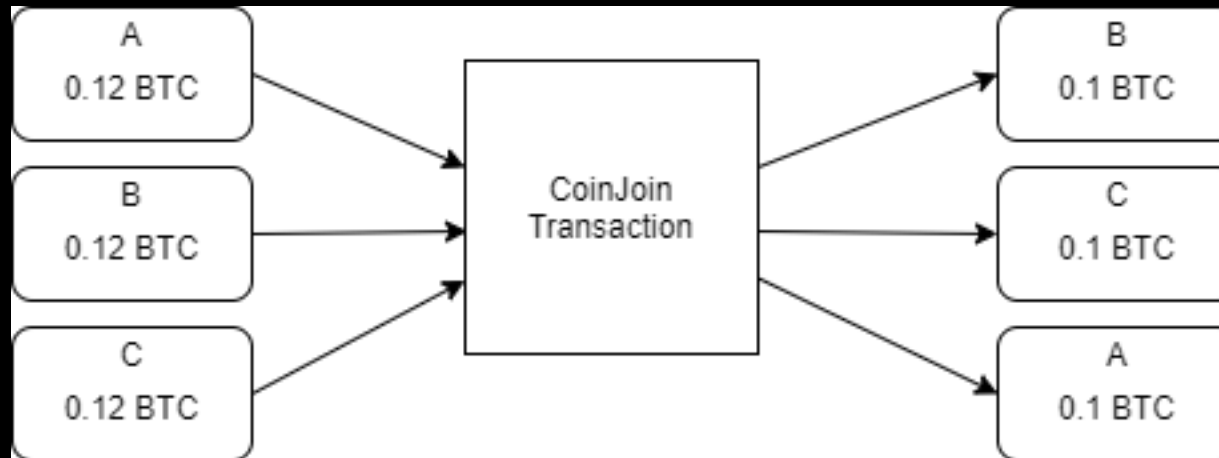
<https://www.justice.gov/archives/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

Bitcoin transaction graph

- Recall, blockchains are public by design
- Each bitcoin has a publicly viewable history
 - Albeit pseudonymous
- Arguably less private in some senses
















Shuffles and Mixes



Other types of cryptocurrencies

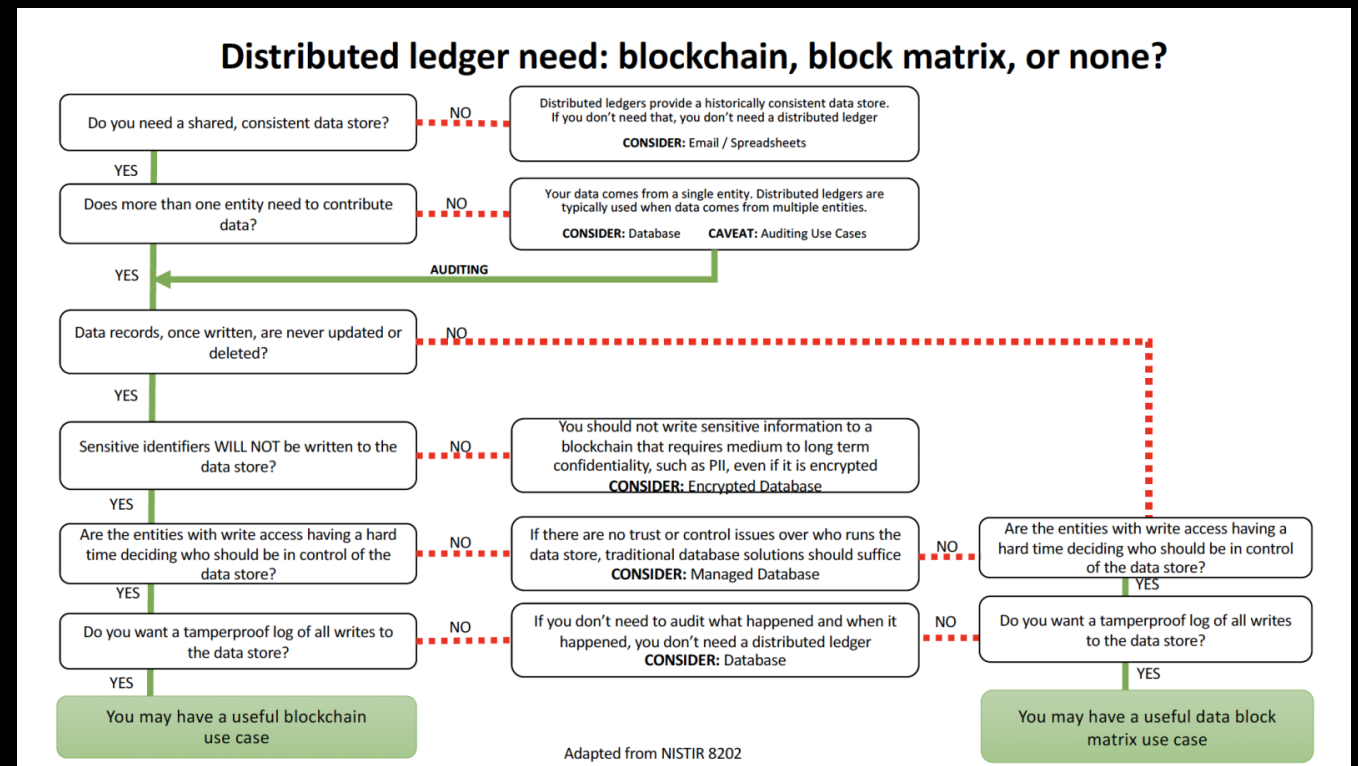
- Can vary in consensus algorithm, level of decentralization, hashrate, blocksize, and more
- Bitcoin-likes
 - Litecoin
 - Dogecoin
- Private
 - Monero
 - Zcash
 - Dash
- More featured
 - Ethereum
 - Proof-of-Stake
 - Smart Contracts
 - Bitcoin also has scripts but they are much more limited

	#	Name	Price	1h %	24h %	7d %	Market Cap 	Volume(24h) 	Circulating Supply 
☆	1	 Bitcoin BTC	\$84,749.77	▲0.31%	▲0.92%	▲3.39%	\$1,682,503,962,449	\$26,089,305,002 309.35K BTC	19.85M BTC
☆	2	 Ethereum ETH	\$1,598.38	▲0.32%	▲1.06%	▼0.35%	\$192,922,139,733	\$14,159,313,358 8.89M ETH	120.69M ETH
☆	3	 Tether USDT	\$0.9994	▲0.00%	▼0.07%	▲0.00%	\$144,731,860,004	\$54,855,015,423 54.86B USDT	144.8B USDT
☆	4	 XRP XRP	\$2.10	▲0.50%	▲1.13%	▲4.33%	\$123,016,655,899	\$2,989,425,304 1.42B XRP	58.33B XRP
☆	5	 BNB BNB	\$586.88	▲0.09%	▲0.79%	▲1.55%	\$82,686,271,375	\$1,407,570,581 2.40M BNB	140.89M BNB
☆	6	 Solana SOL	\$133.85	▲0.64%	▲6.26%	▲16.35%	\$69,124,668,854	\$4,611,940,014 34.72M SOL	516.4M SOL
☆	7	 USDC USDC	\$0.9997	▼0.00%	▼0.04%	▼0.03%	\$60,388,497,925	\$10,098,301,637 10.09B USDC	60.4B USDC
☆	8	 TRON TRX	\$0.2471	▼0.41%	▼2.89%	▲2.70%	\$23,471,239,666	\$728,744,274 2.94B TRX	94.95B TRX
☆	9	 Dogecoin DOGE	\$0.1567	▲0.05%	▲2.05%	▼0.15%	\$23,332,299,794	\$736,963,088 4.71B DOGE	148.88B DOGE
☆	10	 Cardano ADA	\$0.6212	▲0.67%	▲2.29%	▼0.69%	\$21,921,031,485	\$583,286,563 947.23M ADA	35.28B ADA



Blockchain proposed applications

- Cryptocurrencies
- Distributed Apps (dApps)
 - Web 3.0



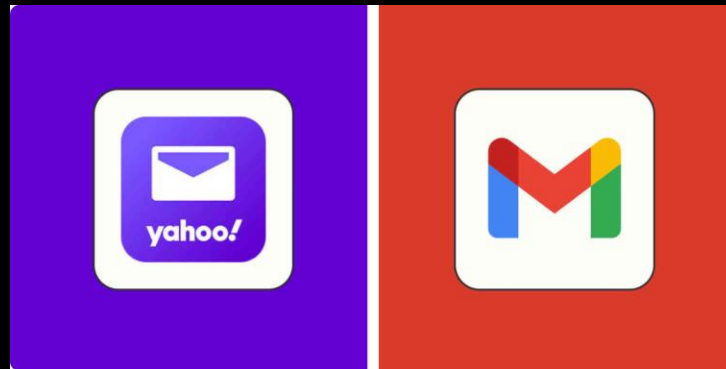
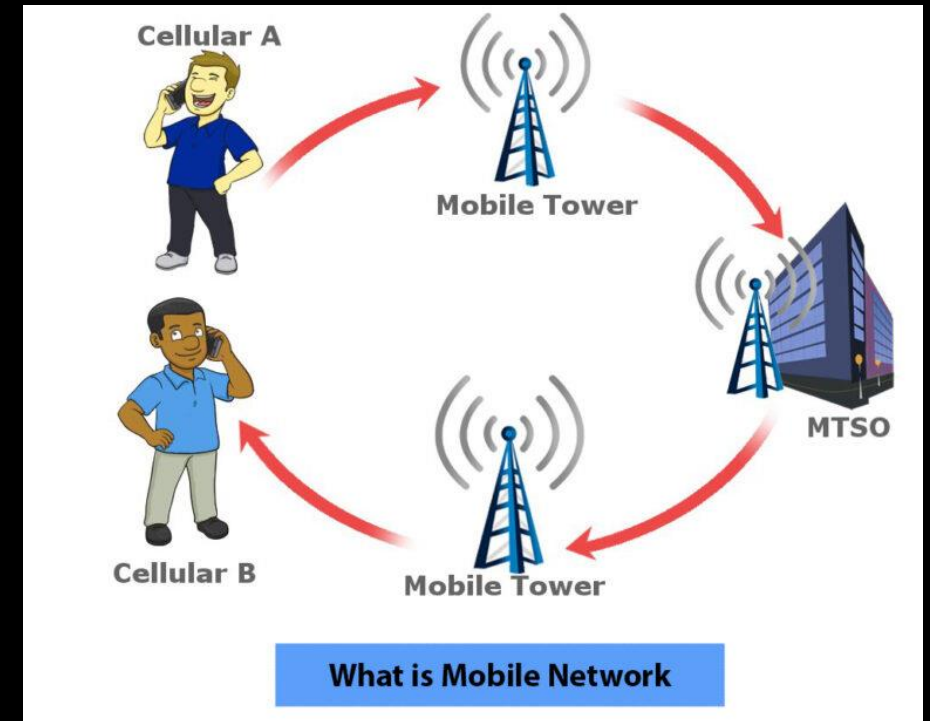
P2P challenges

- Often expects or requires equal participation from everyone to work as intended
 - Tendency to centralize
- Can be complex to coordinate

Federation

- A group of *interoperable* networks that *collectively* agree on *standards of operation*
 - Each network can be otherwise independently managed
- Examples?

Federation Examples



Standards Bodies

- Need to have a way to agree upon standards to avoid *fragmentation*
- Examples
 - NIST
 - MIT X Consortium
 - W3C
 - IETF
 - ITU
- Governance structures can vary

Distributed Social Network

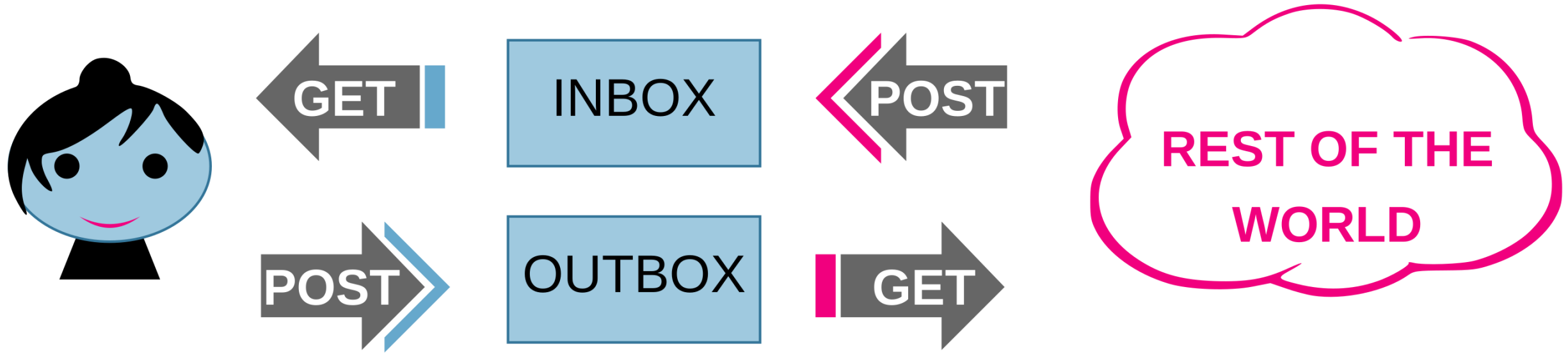
- A set of interoperable social networks
- Distinguishing factor is the portability and lack of a central authority

ActivityPub

- Standard for decentralized social networking developed by W3C
- Is both client-to-server and server-to-server
- Comprised of Objects, Actors, and Activities
- Used by
 - Mastodon
 - Threads
 - Lemmy
 - WordPress

actor reads
incoming messages

send messages
to actor (federation!)



actor sends
messages / post content

outside world can read
messages from actor

Users

```
{
  "@context": ["https://www.w3.org/ns/activitystreams",
    {"@language": "ja"}],
  "type": "Person",
  "id": "https://kenzoishii.example.com/",
  "following": "https://kenzoishii.example.com/following.json",
  "followers": "https://kenzoishii.example.com/followers.json",
  "liked": "https://kenzoishii.example.com/liked.json",
  "inbox": "https://kenzoishii.example.com/inbox.json",
  "outbox": "https://kenzoishii.example.com/feed.json",
  "preferredUsername": "kenzoishii",
  "name": "石井健蔵",
  "summary": "この方はただの例です",
  "icon": [
    "https://kenzoishii.example.com/image/165987aklre4"
  ]
}
```

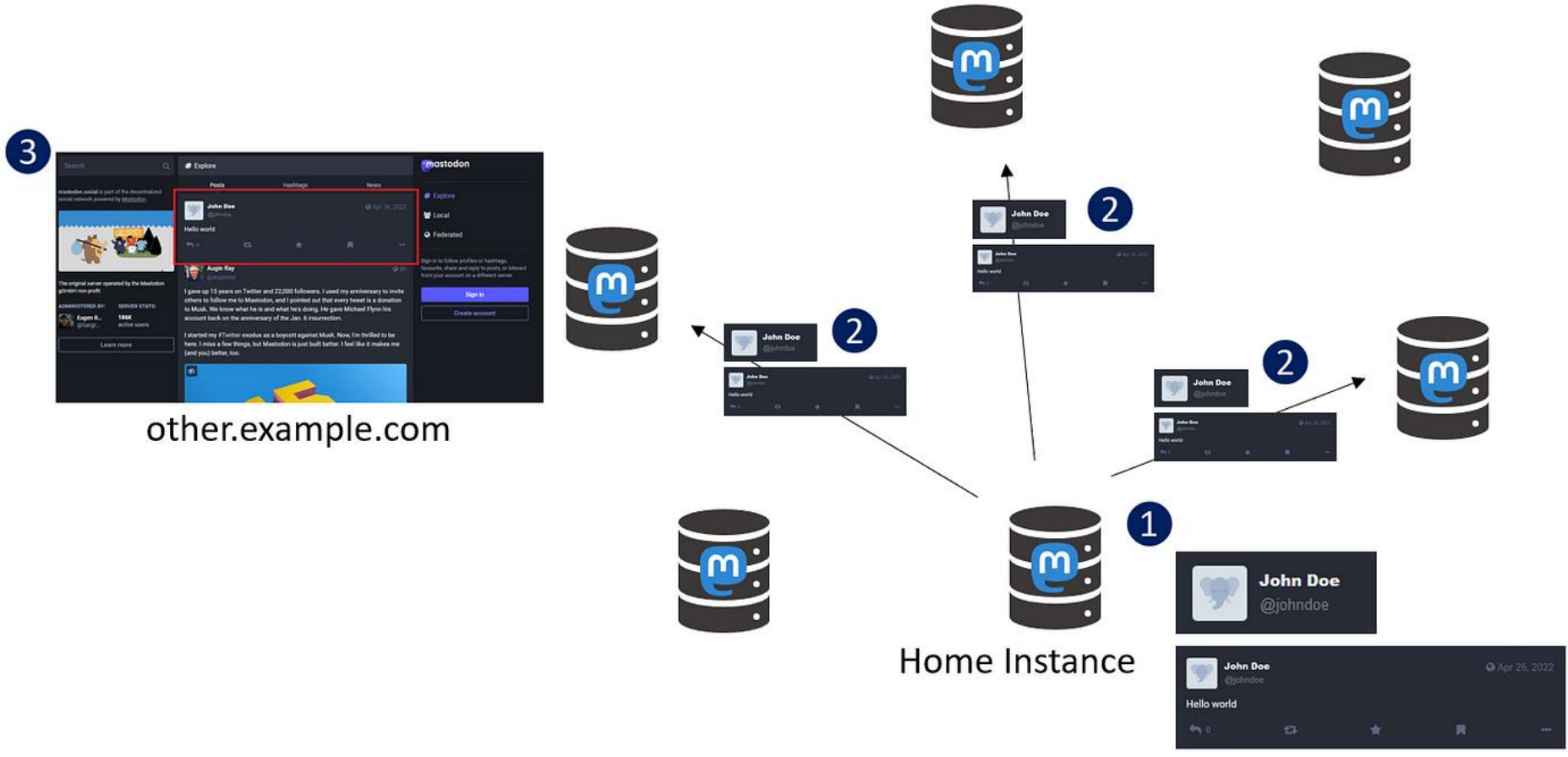
Objects

```
{
  "@context": ["https://www.w3.org/ns/activitystreams",
    {"@language": "en-GB"}],
  "id": "https://rhiaro.co.uk/2016/05/minimal-activitypub",
  "type": "Article",
  "name": "Minimal ActivityPub update client",
  "content": "Today I finished morph, a client for posting
ActivityStreams2...",
  "attributedTo": "https://rhiaro.co.uk/#amy",
  "to": "https://rhiaro.co.uk/followers/",
  "cc": "https://e14n.com/evan"
}
```

Activities

```
{
  "@context": ["https://www.w3.org/ns/activitystreams",
    {"@language": "en"}],
  "type": "Like",
  "actor": "https://dustycloud.org/christine/",
  "summary": "Christine liked 'Minimal ActivityPub update client'",
  "object": "https://rhiaro.co.uk/2016/05/minimal-activitypub",
  "to": ["https://rhiaro.co.uk/#amy",
    "https://dustycloud.org/followers",
    "https://rhiaro.co.uk/followers/"],
  "cc": "https://e14n.com/evan"
}
```

Mastodon

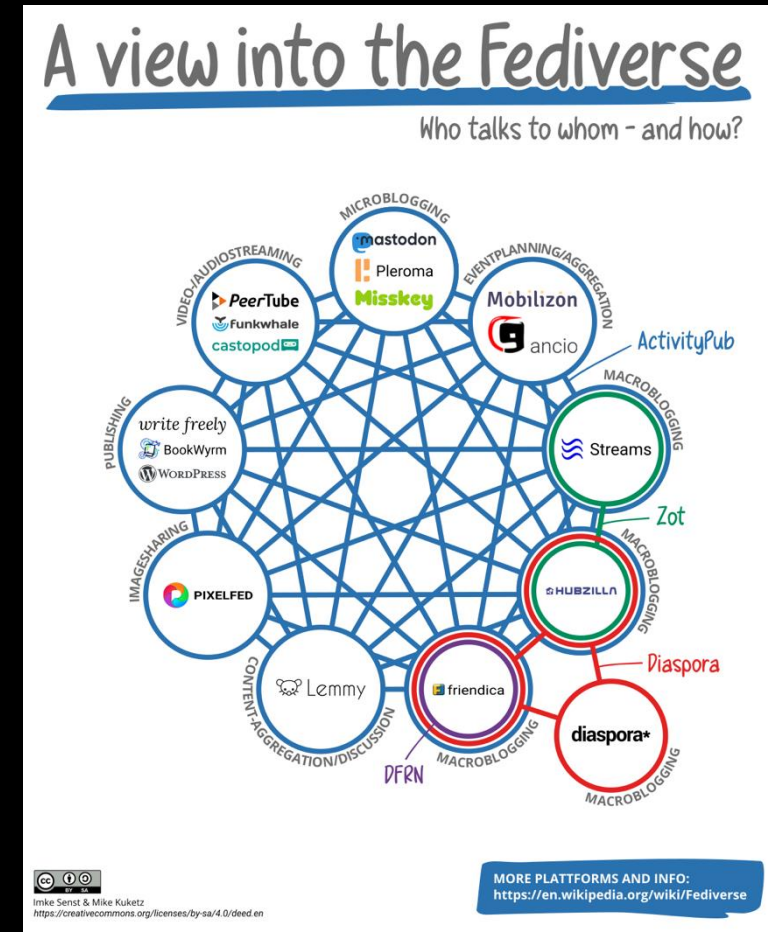


Mastodon

- Users join a specific server
- Each server can enforce its own rules, norms, and moderation
- ActivityPub allows for fetching and interacting with content from other servers

Fediverse

- Fun consequence of ActivityPub is any ActivityPub server is interoperable
 - Not just Mastodon <-> Mastodon



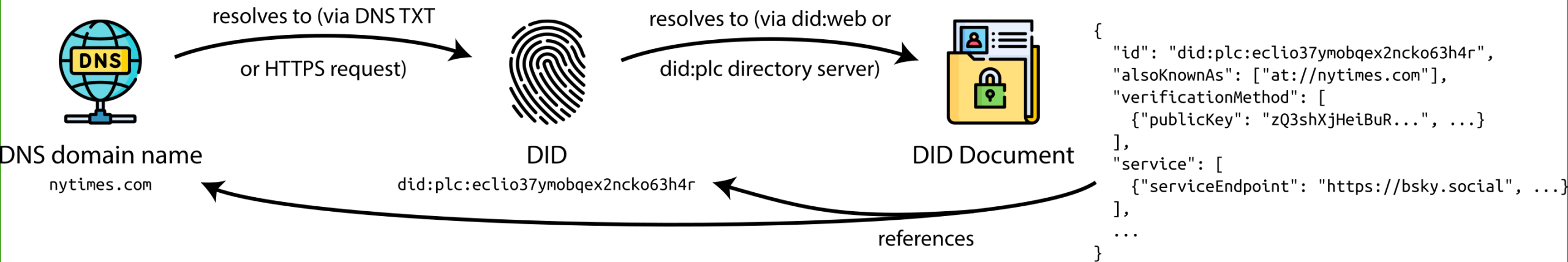
Considerations with Federation

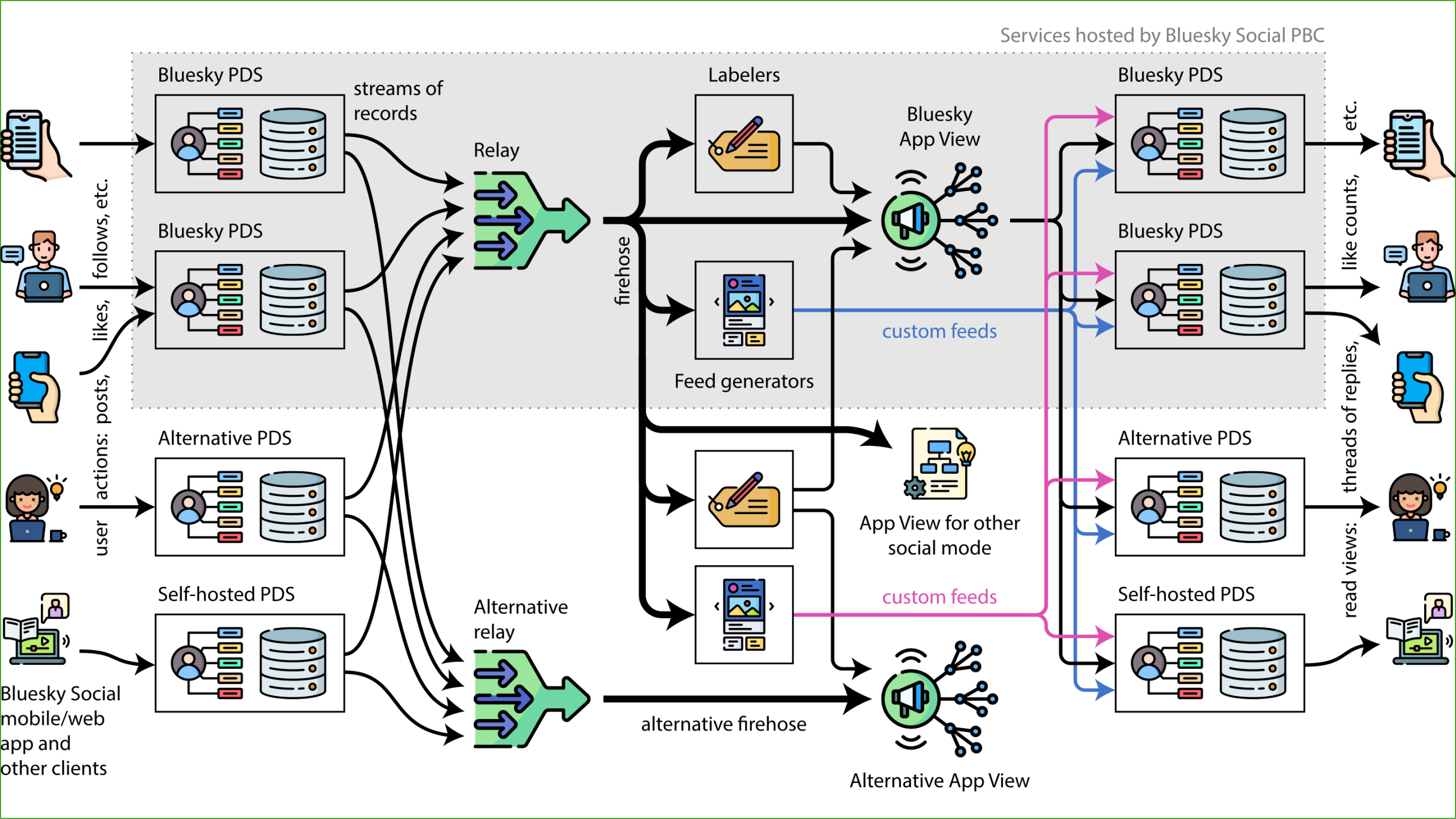
- Privacy
- Trust and Safety
- Security Issues
- Forks and Defederation
- Funding and Development

AT Protocol

- Alternative distributed social networking protocol developed by Bluesky
 - Plan is to transfer management to the IETF
 - Refers to its set of interoperable applications as the ATmosphere
- Originated as part of an internal research initiative within Twitter to explore decentralizing the network
- Rather than relying on instance specific servers, works through many microservices
- Not naturally compatible with the Fediverse but can interoperate through the use of a *bridge*

Identity





Next Time

DRM, Right to Repair, and Open Source