STRĀTUMN

CRYPTO NIGHTS №2

BYZANTINE FAULT TOLERANCE AGAINST CENSORSHIP

ANTON ZUENKO

Why to censor?

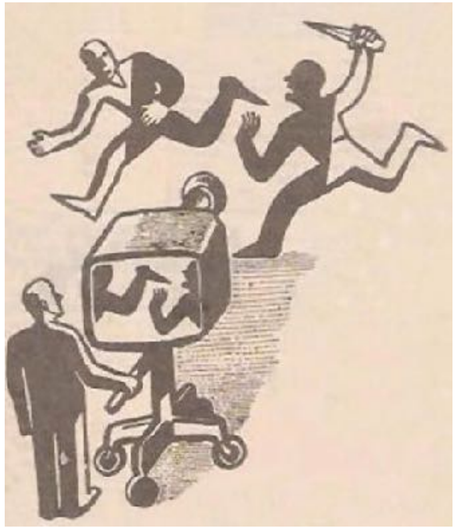
- Censorship != Information should be free

- To protect moral values
  - violence and nudity
- To ensure free market / competition
  - confidential information, military secrets
- Protect ideological integrity
  - persecution of heretics, dissidents; book burning

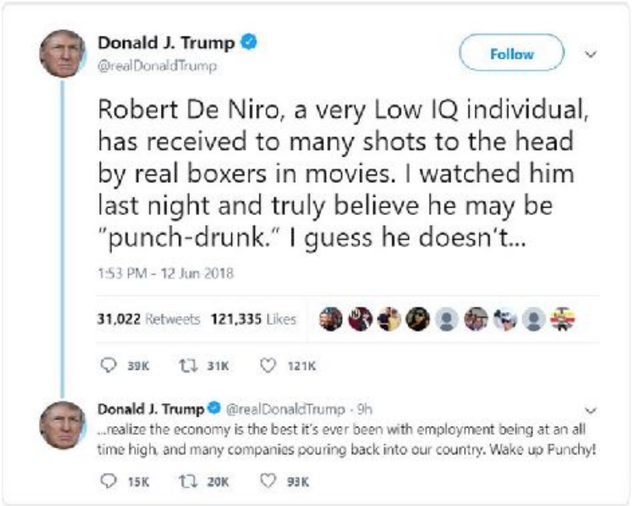
@latuffCartoons

Censorship in news media

- Before publishing
  - 😶 Silencing: some storied not covered
  - ⚖️ Bias: only one side of the story
- After publishing
  - ✏️ Alteration: modification of published content
  - 🚫 Removal: “we didn’t say that”



RT covering Syria



One of 350+ deleted Trump tweets

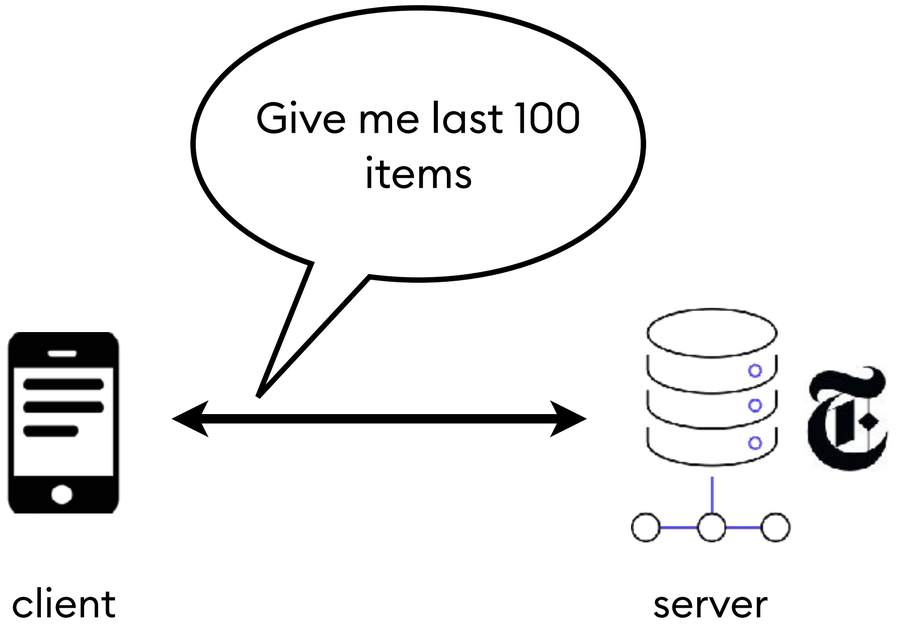
Censorship in many cases contradicts with the values of journalism: independence, impartiality, accountability, ...

“Who controls the past controls the future: who controls the present controls the past”

George Orwell

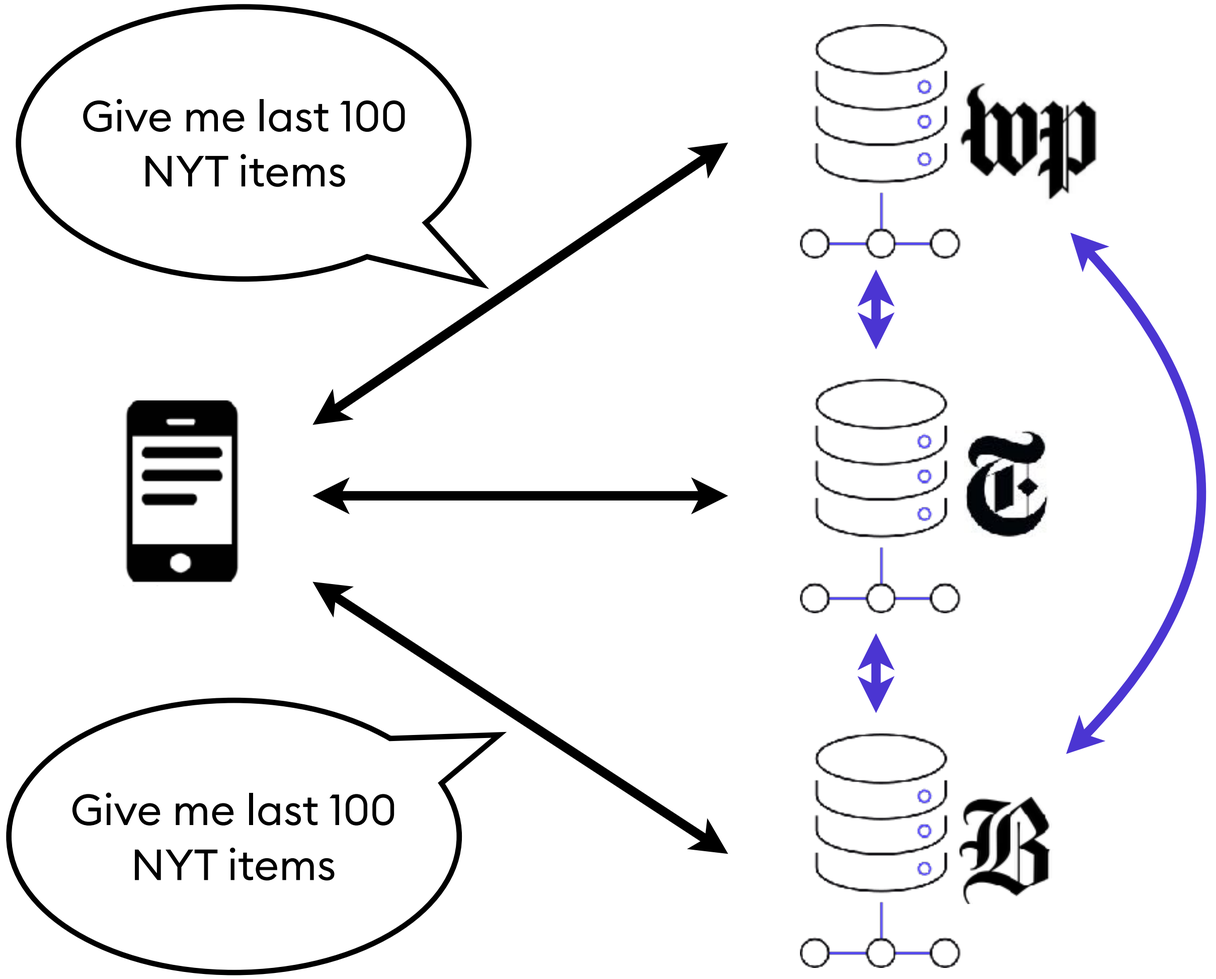
Client-server model

- Fetch each time – provider decides what to return
- No local copies – easier to control the content (delete, modify)
- Web feed (RSS / Atom) partially solves the issue



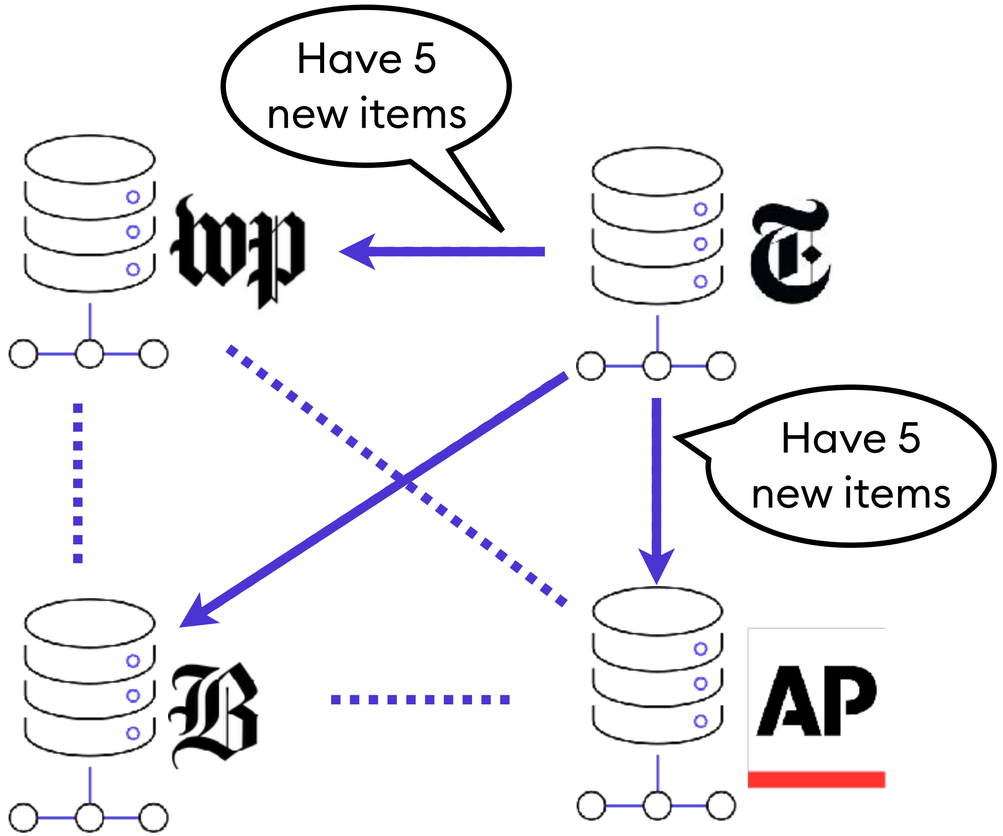
Client-network model

- Fetch **same** data from multiple independent providers
- Compare and accept only when enough replies are received
- Each provider hosts data of all other providers within the network
- Requires synchronisation between the providers



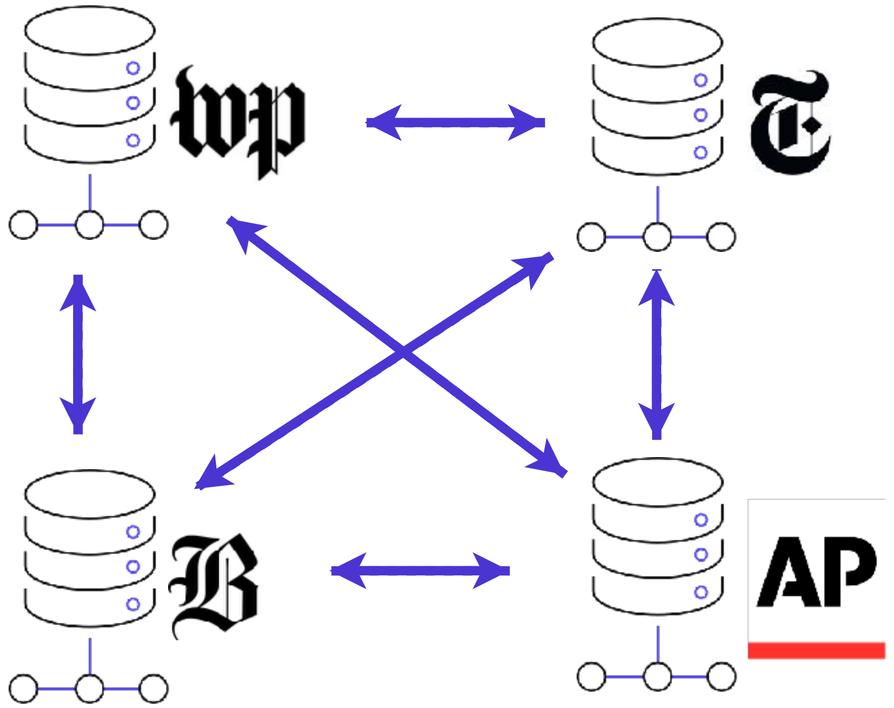
Push protocol

- Providers retain direct peer-to-peer connections in a flat network
- Each provider pushes new data onto other providers' servers
- Push-only interface doesn't allow to delete / modify already pushed data
- Works well when there's no cross-references



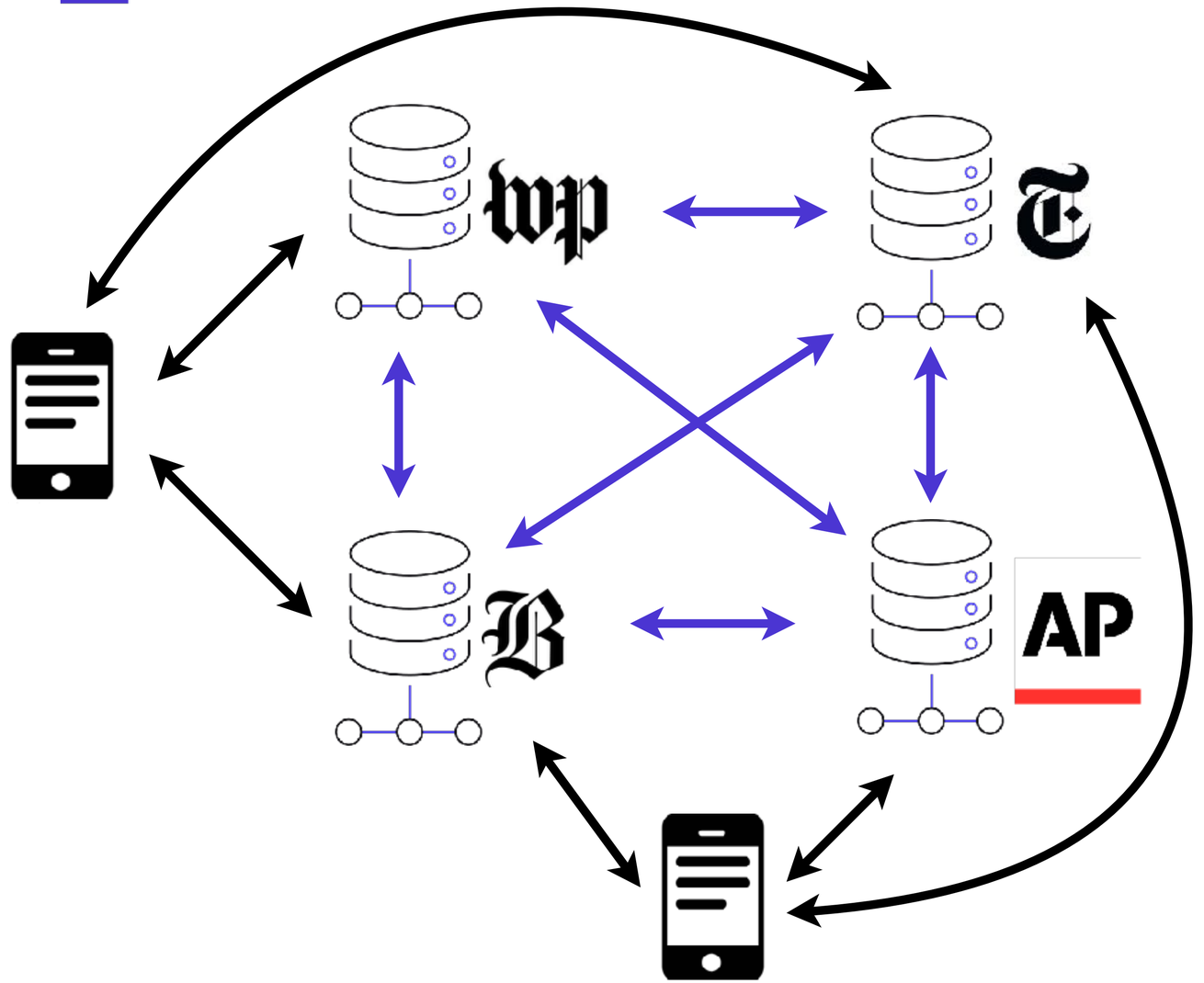
Cross-referencing requires consensus

- Cross-reference
  - NYT: “According to the story published by Associated Press, […]”
- To retain censorship-resistance, “story” should reference a data item in the same network
- NYT has the item, since AP pushed it
  - But NYT has to be sure that everybody else also has the same item
- In push protocol nothing prevents AP to push different items to different providers
- Therefore, NYT should query other providers to ensure the consistency of the referenced item
- Push protocol should be replaced with **consensus protocol**



Full picture

- Members of the network run consensus protocol to synchronise data,
- Clients connect to multiple servers to fetch data they are interested to,
- Clients display data only when the majority of the providers say the same thing,
- News items may contain references to previously published news items, possibly from different providers,
- Referenced data is obtained the similar way by querying multiple providers.



Summary

Incentives

- Users are incentivised to use the network as it provides “immutable” content
- Media providers are incentivised to join the network as they earn points of credibility

Issues

- Performance – client has to fetch same data multiple times
- Performance – BFT consensus protocol isn’t quite scalable
- Decentralised network orchestration (governance) – add / remove participants
- Business model – whom to pay for the content?
- Content sharing in the context of data protection laws

Thanks for your attention!