

# 4git

## Practical decentralized architecture for deliberative applications

Petar Maymounkov

Protocol Labs / Microsoft Research / GitHub / RadicalXChange

Austin Akers, Jason Entenmann, Leon Erichsen, Siddhant Kasat, Evan Miyazono,  
Sangeet Parashar, Kasia Sitkiewicz, Shivani Thakur, Glen Weyl

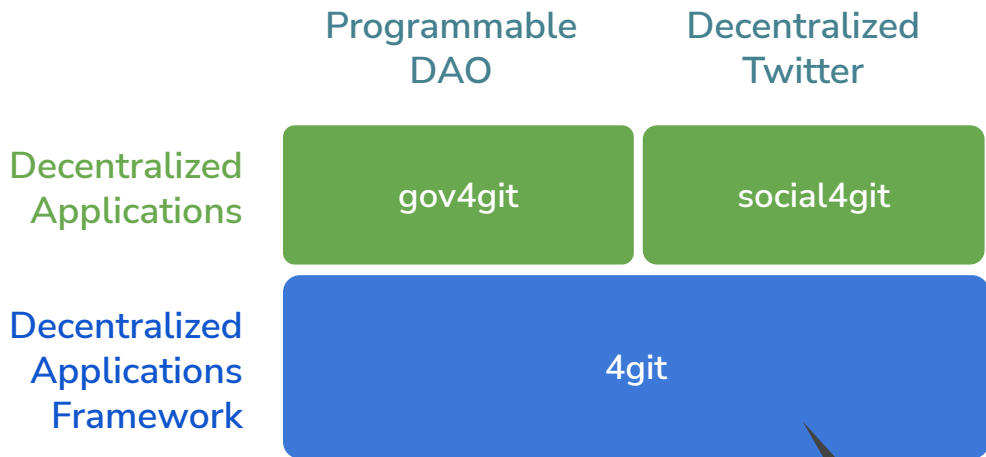
# Deliberative applications for democracy

## Governance

- polling, voting, policymaking

## Discourse

- social media, blogging, chat

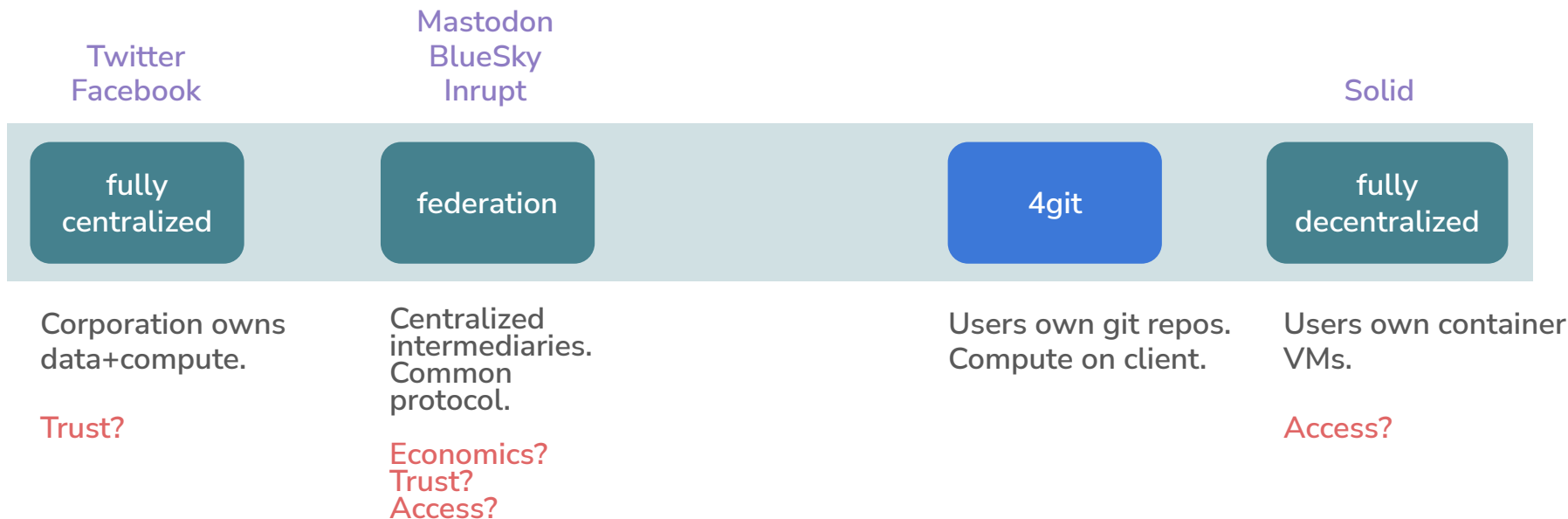


This talk!

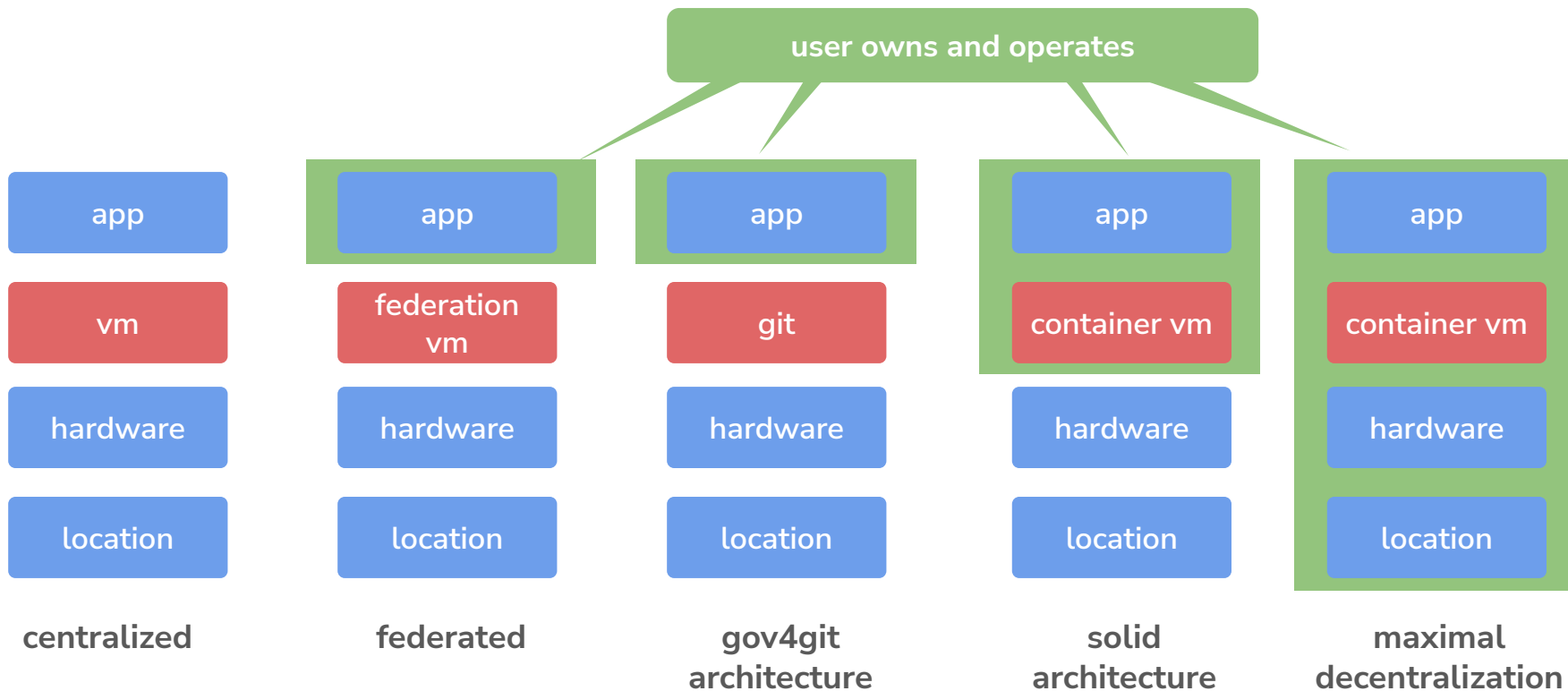
# A crux of designing decentralized software

Tug-of-war between **ownership** and **responsibility** (for the end users)

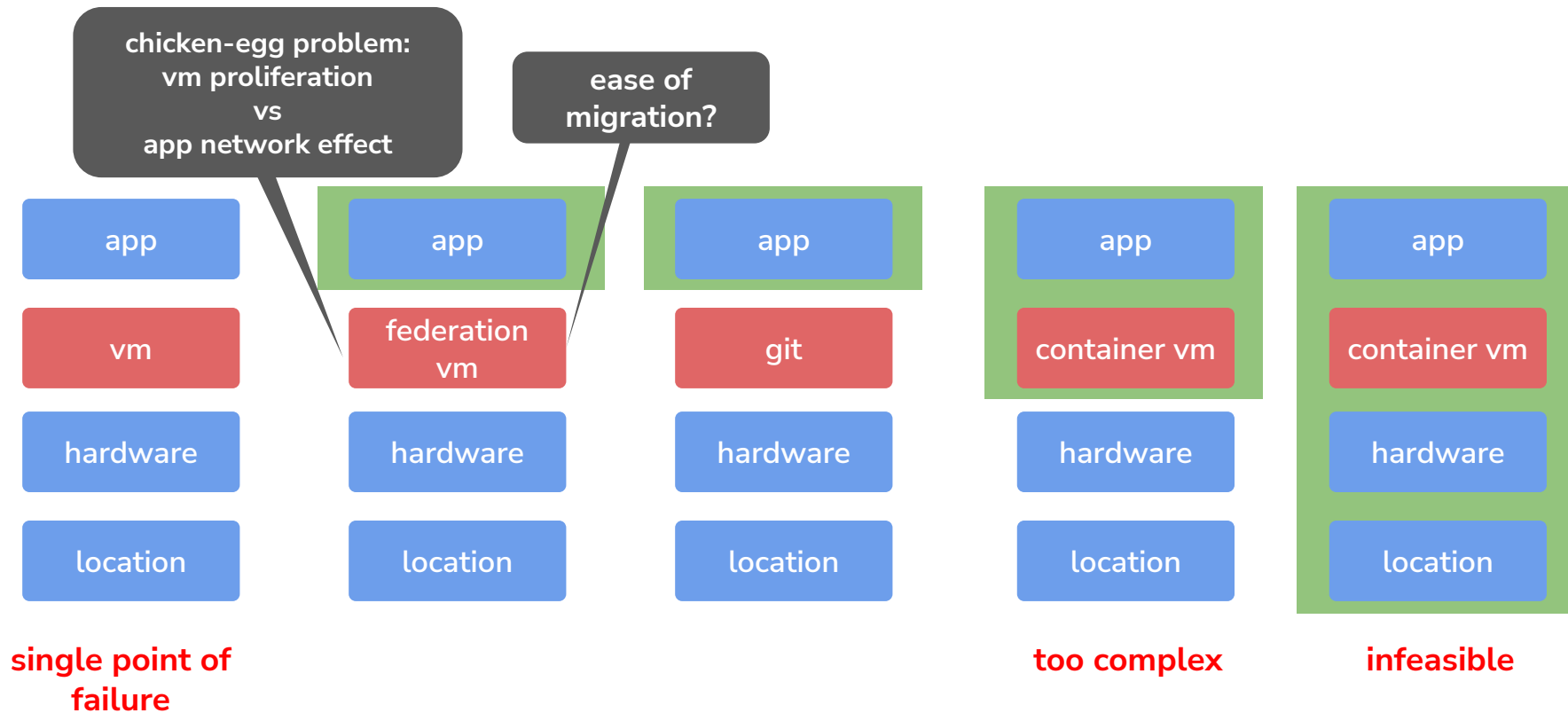
- Users desire to own their data+compute
- Users are responsible to operate the infra that holds their data+compute



# The spectrum of decentralization stacks



# The spectrum of decentralization stacks



# Practical technical requirements

## Deployable by non-technical users

- Not all open source communities are comprised of engineers (journalists, designers)

## Zero (financial) cost

- Developing world, war/disaster zones, authoritarian regimes, minors

## Commodity hardware

- Ditto

## Disconnected from the public Internet

- Government censorship of public services (e.g. blockchains, federation, Twitter)

## Easy and rapid application development

- Programmable with simple high-level languages (scripting, Python, etc.)

# Decentralized infrastructure for apps

## Abstract requirements for decentralized applications

- Identity (social media)
- Communication (social media)
- Trusted computation (governance, DAOs)
  - Replicated state machine
  - Transparent program
  - Transparent state
  - Assured correct execution

# High-level architecture

## Tenet

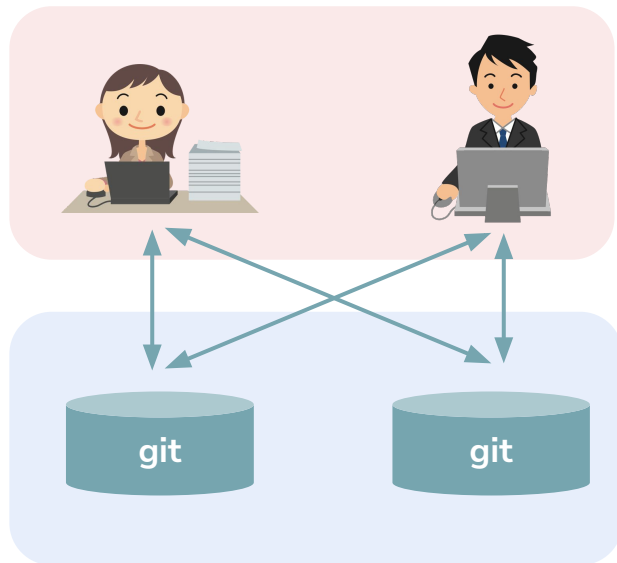
- Persistent infra (i.e. backend) is standard git server (repo)
- No other persistent infra, by design requirement!

## Storage

- Git backend

## Compute

- On client (browser, mobile, command-line)
- Light cron job (GitHub actions, serverless, mobile, home)

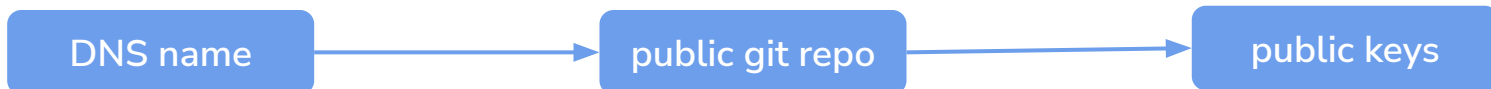




# Identity

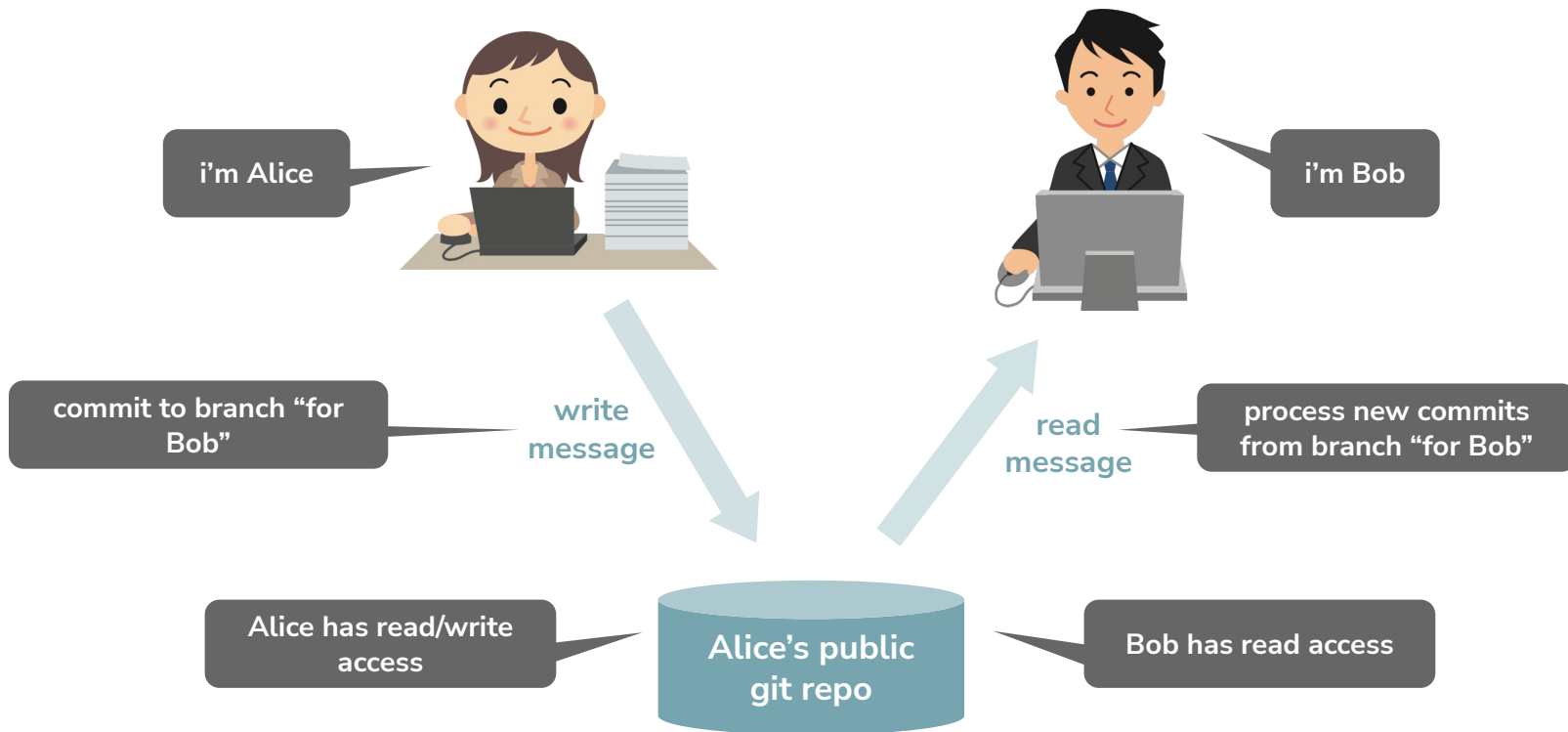
Every user provisions/owns infra:

- public git repo (owner writes, everyone reads)
- private git repo (owner writes / owner reads)



github.com/petar/gov4git.id  
maymounkov.org  
maymounkov.eth

# Solicited communication (1 of 2)



# Solicited communication (2 of 2)

## Latency

200 ms (Web 2.0) < 1 sec (gov4git) < 30 sec (Web 3.0, DWeb, blockchains)

## Semantics

- pull mechanism → solicited communication only (i.e. permissioned messaging)
- captures social media (e.g. Twitter), permissioned community apps (e.g. DAOs)
- does not capture unsolicited comms apps (e.g. email)

## Do not confuse

- permission/less apps (e.g. DAOs)
- permission/less infrastructure (e.g. underlying blockchain)

# Trusted computation (1 of 3): Consensus

## Proof-of-work blockchains (permissionless)

- Bitcoin, Ethereum, Filecoin, ...

## Byzantine blockchains (permissioned)

Use Byzantine Fault-tolerant State Machine Replication (BFT SMR)

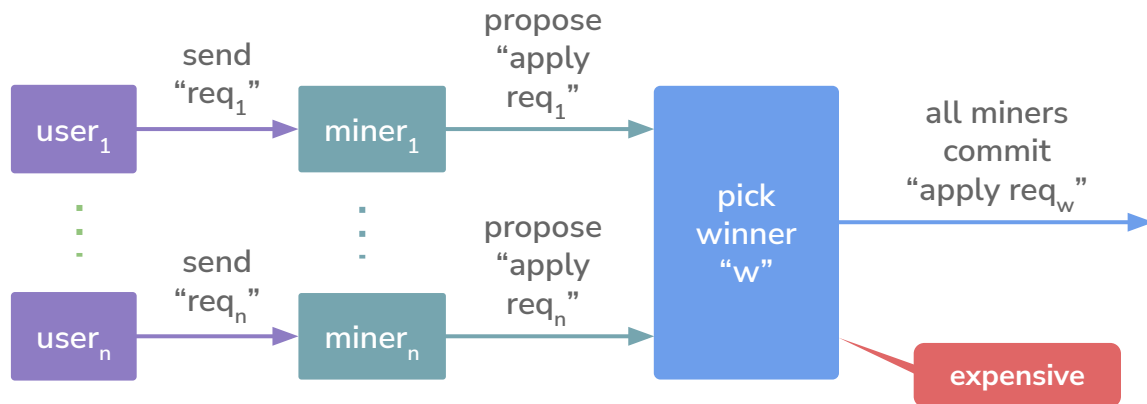
- partial synchronous model
  - PBFT < Tendermint < HotStuff < ...
- synchronous model
  - Practical Synchronous Byzantine Consensus [Ren, et al. 2017]

## Human-centric deliberative applications are not latency-sensitive

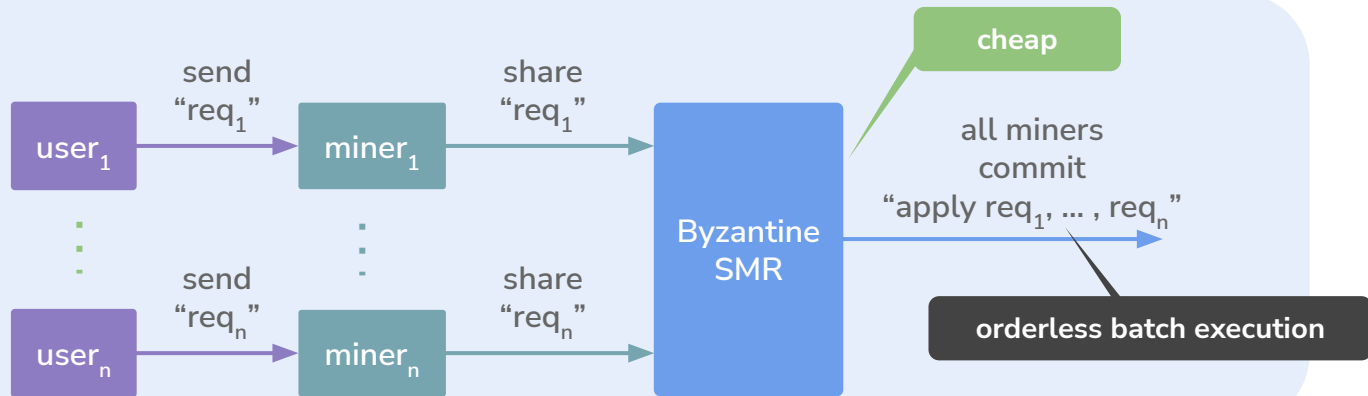
- One hour block finalization suffices for voting and polling

# Trusted computation (2 of 3): API

proof-of-work  
blockchains



Byzantine  
blockchains



# Trusted computation (3 of 3): Order and conflicts

Our community blockchains host a single-application

Conflicts between requests from **the same user**

- Users apply sequence numbers on their own requests (persisted in their git)

Conflicts between requests from **different users**

- Deferred to the application (batch processing of all requests in a round)

# Developer experience

VMs require custom languages or compiler plugins. Complex moving targets!

- Solidity, WASM, Rust, Fe, AssemblyScript, etc.

Our blockchain interfaces with applications through the file system

- State of the blockchain is a file system (git commit)
- Applications modify the state (using any programming technology)
- Blockchain layer processes state changes