Anonymous Forums with Reputation

Ian Miers, Maurice Shih, Michael Rosenberg, **Hari Kailad**

Current-day Forums

Pseudonymous: allows tracking of users

Anonymous without state: Can't moderate users

Anonymous Blocklisting

Prior Work: *BLAC*, *Snark Block*, *PEREA*

Can we have a practical protocol for an anonymous forum with moderatable user state?

(coming soon to an eprint near you)

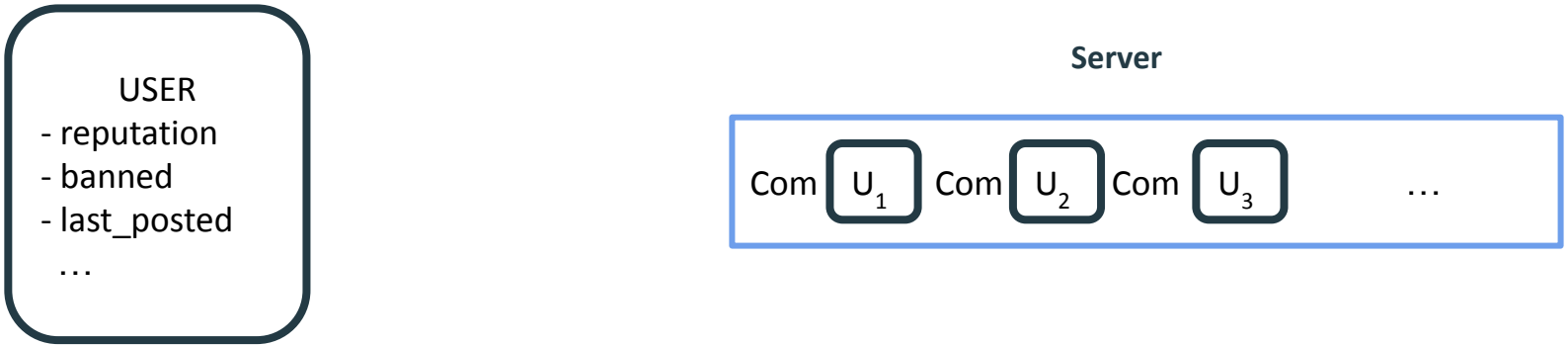
Zk-callbacks: A framework for anonymous reputation systems

- Builds upon Zerocash-like systems
- Anonymous forums with moderation
- Arbitrary State

Made possible due to cryptography™ (specifically SNARKS)!

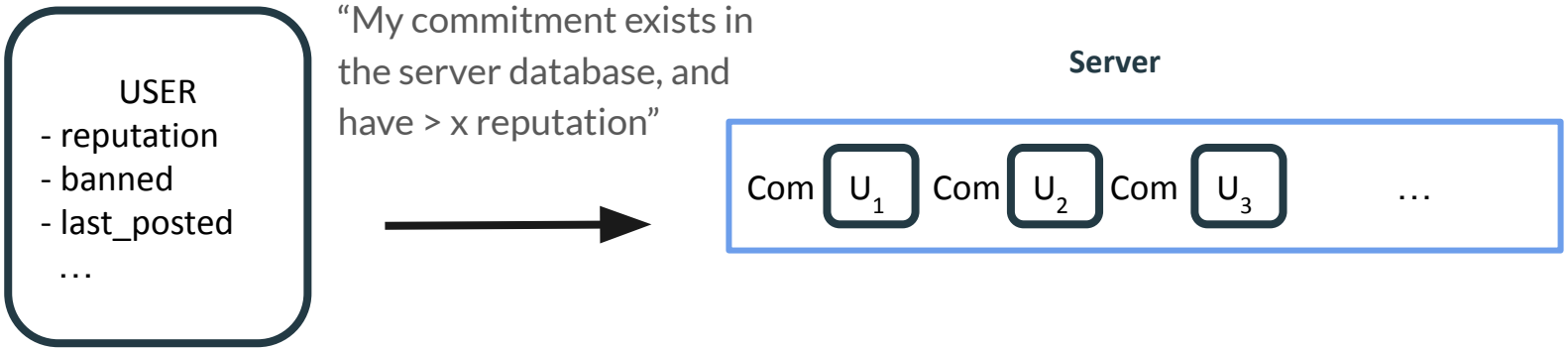
Anonymous Forum: The flow

User stores their state, server stores commitments to the state



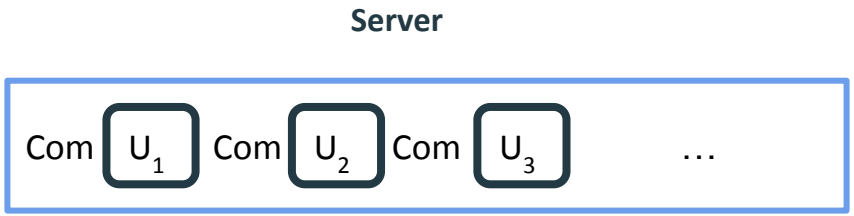
Anonymous Forum: The flow

Can prove statements about the state using zk-SNARKS



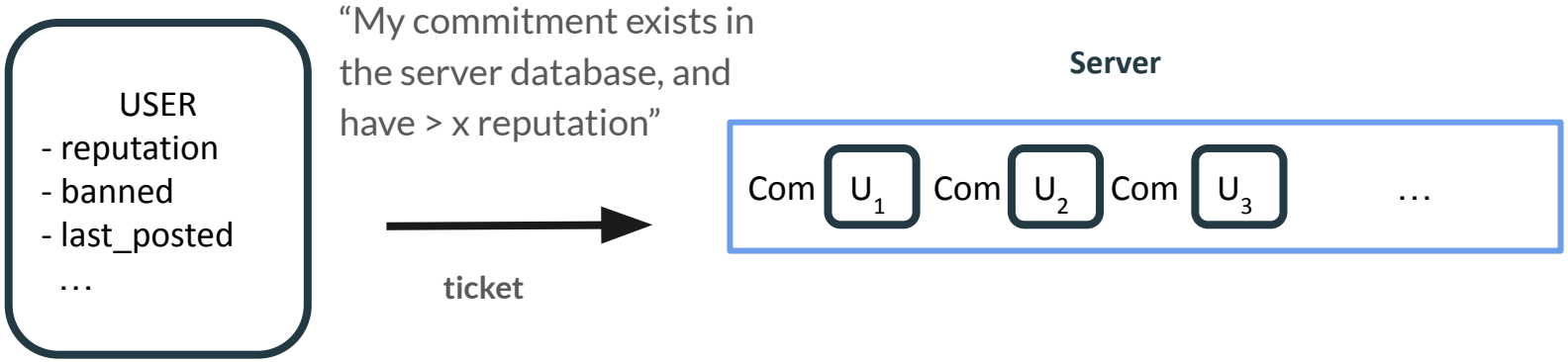
Problem: How to force users to update reputation?

User makes a bad post on Wikipedia or Reddit – how do we force users to accept **negative** feedback?



Reputation: Accepting server feedback

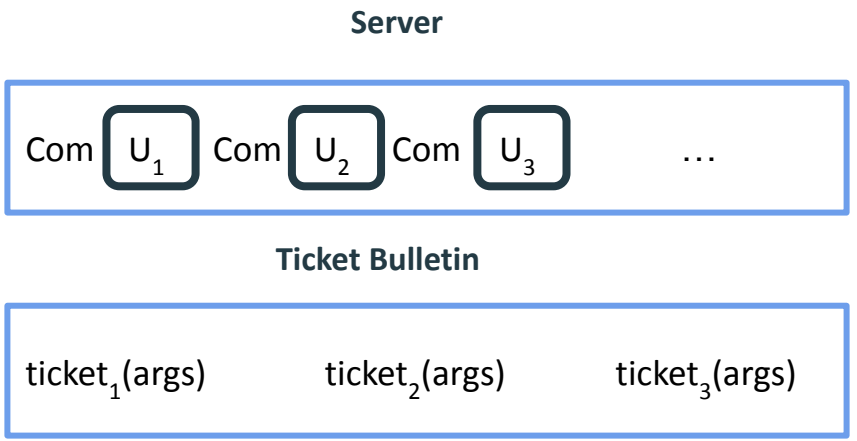
On server interaction: User sends a *ticket* to the server for a one time use.



Reputation: Accepting server feedback

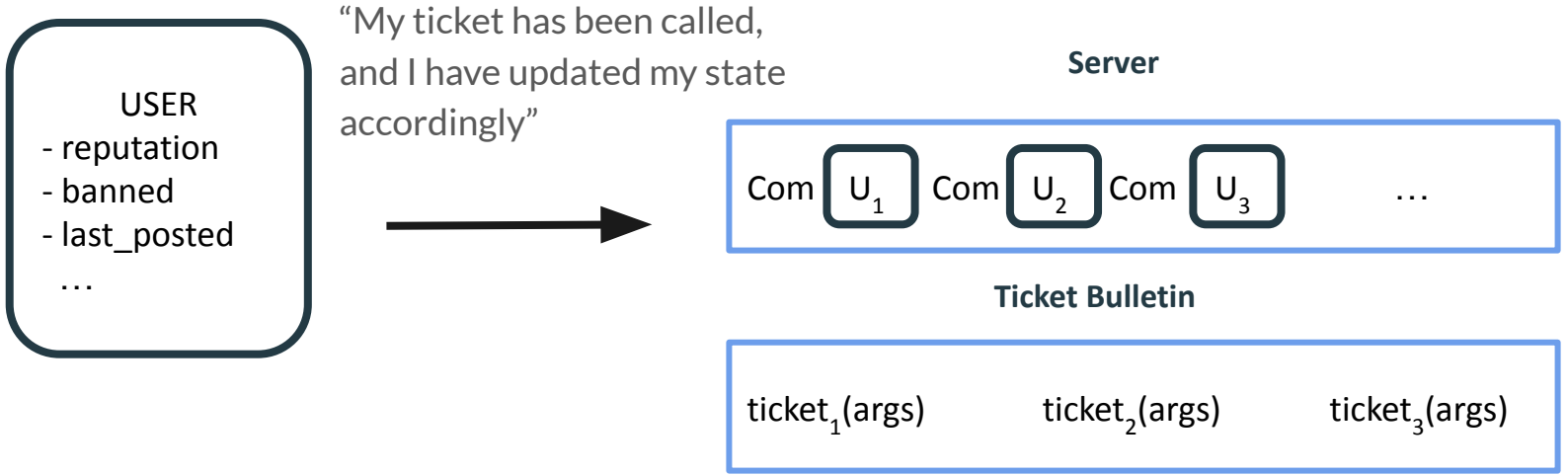
Updating reputation: The server can then update the state by “calling” this ticket, or posting it publicly.

USER
- reputation
- banned
- last_posted
…



Reputation: Accepting server feedback

The user is then forced to update their state by giving a proof of method update if their ticket is in the bulletin.



Applications

Currently WIP: Generic library for arbitrary state updates

- Allows any function to be called on the user state

Also WIP: Anonymous forum for students

- Uses zk-email for membership to show you are a student

Future Work

Private State: Users currently see the full state – Fingerprinting, Ad fraud prevention

Adding Efficient Folding: Improves the efficiency of constructing user proofs

| ***Whistleblowing*** | ***PrivacyPass*** | ***Cryptocurrency reputation*** | ***Ad-fraud prevention*** |

Questions and Things that I can put if I have time

Is there a need or a market for fully anonymous forums with reputation?

- How many people actually care about anonymity?

In practice the forum for students is slightly annoying

- requests are sent through Tor (so IP correlation isn't a thing)
- weird login flow (need to get a zk-email proof)
- Needs to be an application (proving in zk on the web using wasm is SLOW)

Are there other uses for zk-callbacks and arbitrary state calls?