Reputable List Curation from Decentralized Voting

Crites et al. (2020)

Konstantinos Chousos, ALMA

27 February, 2026

National Technical University of Athens (NTUA)

Motivation

Motivation

- Goal: Decentralization

Motivation

- Goal: Decentralization
  - Result: Lack of Trusted Third Parties (TTP)

Motivation

- Goal: Decentralization
  - Result: Lack of Trusted Third Parties (TTP)
- Problem: TTPs sometimes needed

Motivation

- Goal: Decentralization
  - Result: Lack of Trusted Third Parties (TTP)
- Problem: TTPs sometimes needed
- Solution: **Token-Curated Registries** (TCRs)

Contributions

First formal treatment of TCRs. Namely:

Contributions

First formal treatment of TCRs. Namely:

- First formal definition
- First *provably secure* TCR model

Contributions

First formal treatment of TCRs. Namely:

- First formal definition
- First *provably secure* TCR model

Properties offered:

- Vote secrecy
- Dispute freeness
- Self-tallying

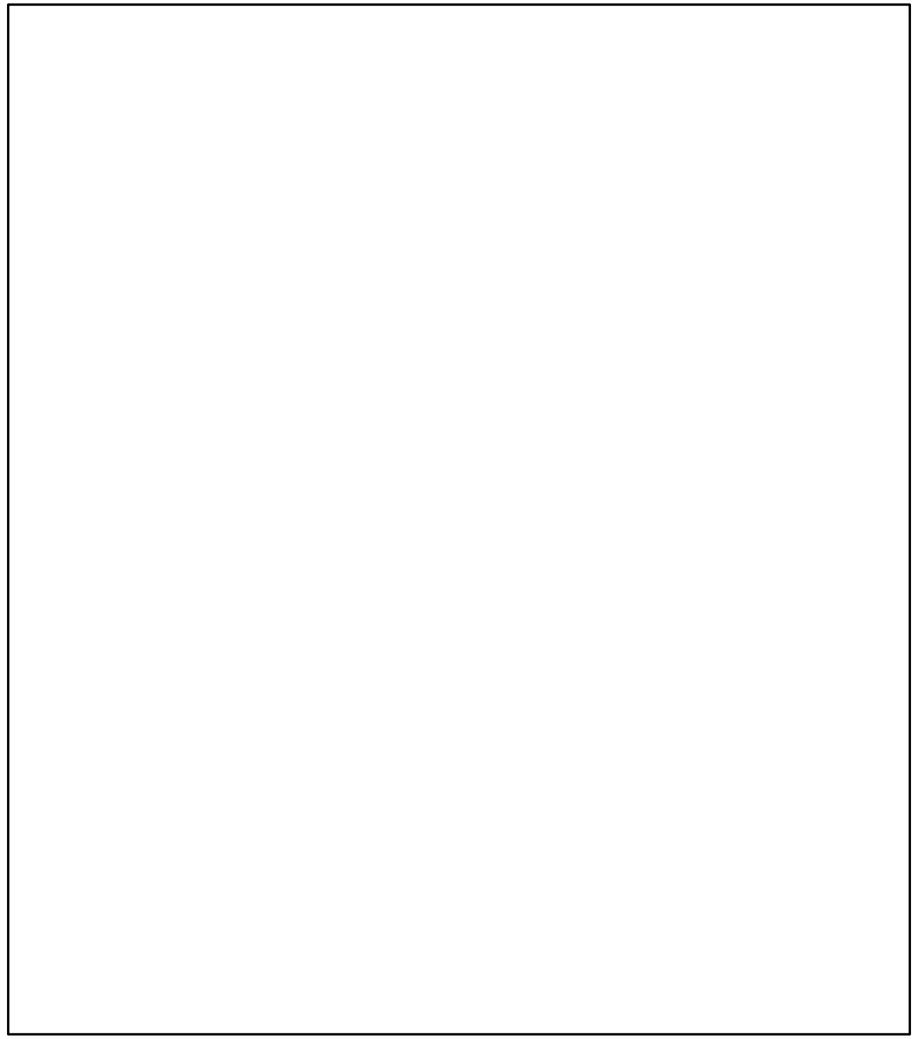
F. Hao, P. Ryan, and P. Zieliński, "Anonymous voting by two-round public discussion," IET Information Security, vol. 4, no. 2, pp. 62–67, Jun. 24, 2010, issn: 1751-8709, 1751-8717. doi: 10.1049/iet- ifs.2008.0127.

Background

- Blockchains
  - Turing-complete scripting language
- Smart Contracts
  - Deterministic
  - Transparent
- Token-Curated Registries

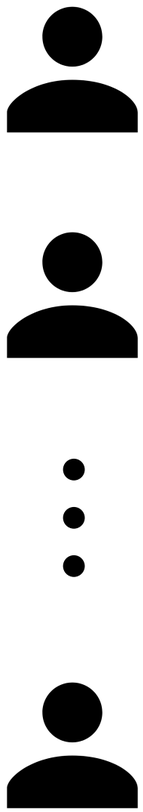
TCR Workflow

Contract (TCR)



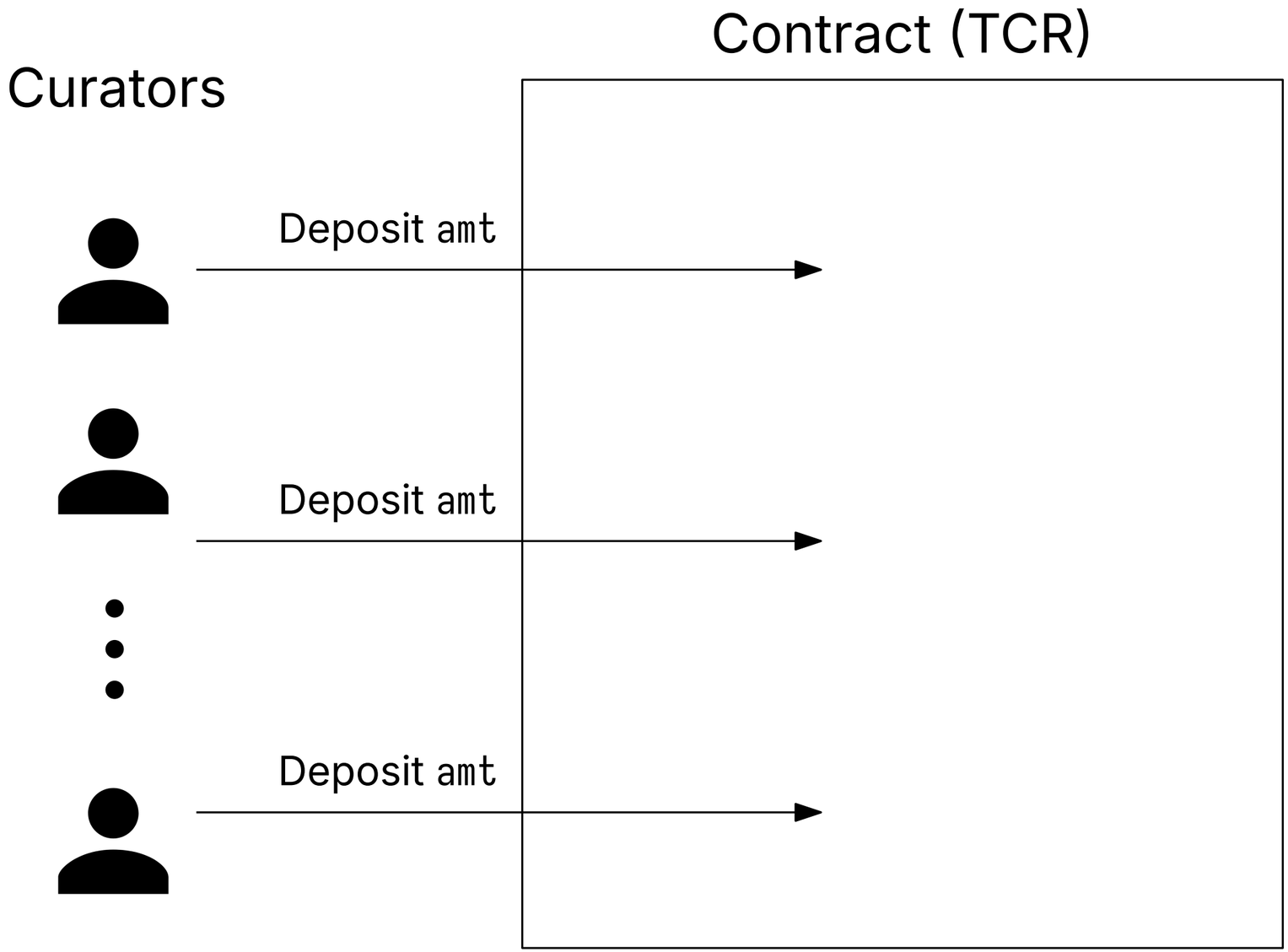
TCR Workflow

Curators



Contract (TCR)

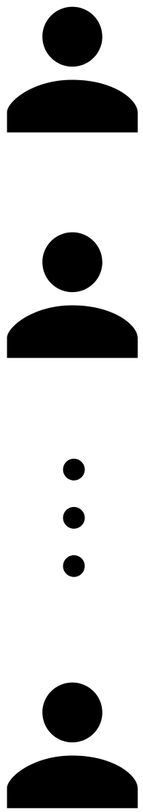
TCR Workflow



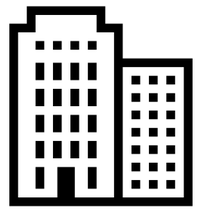
TCR Workflow

Contract (TCR)

Curators



Service



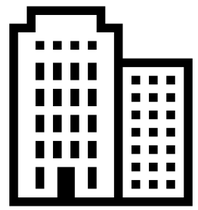
Apply

TCR Workflow

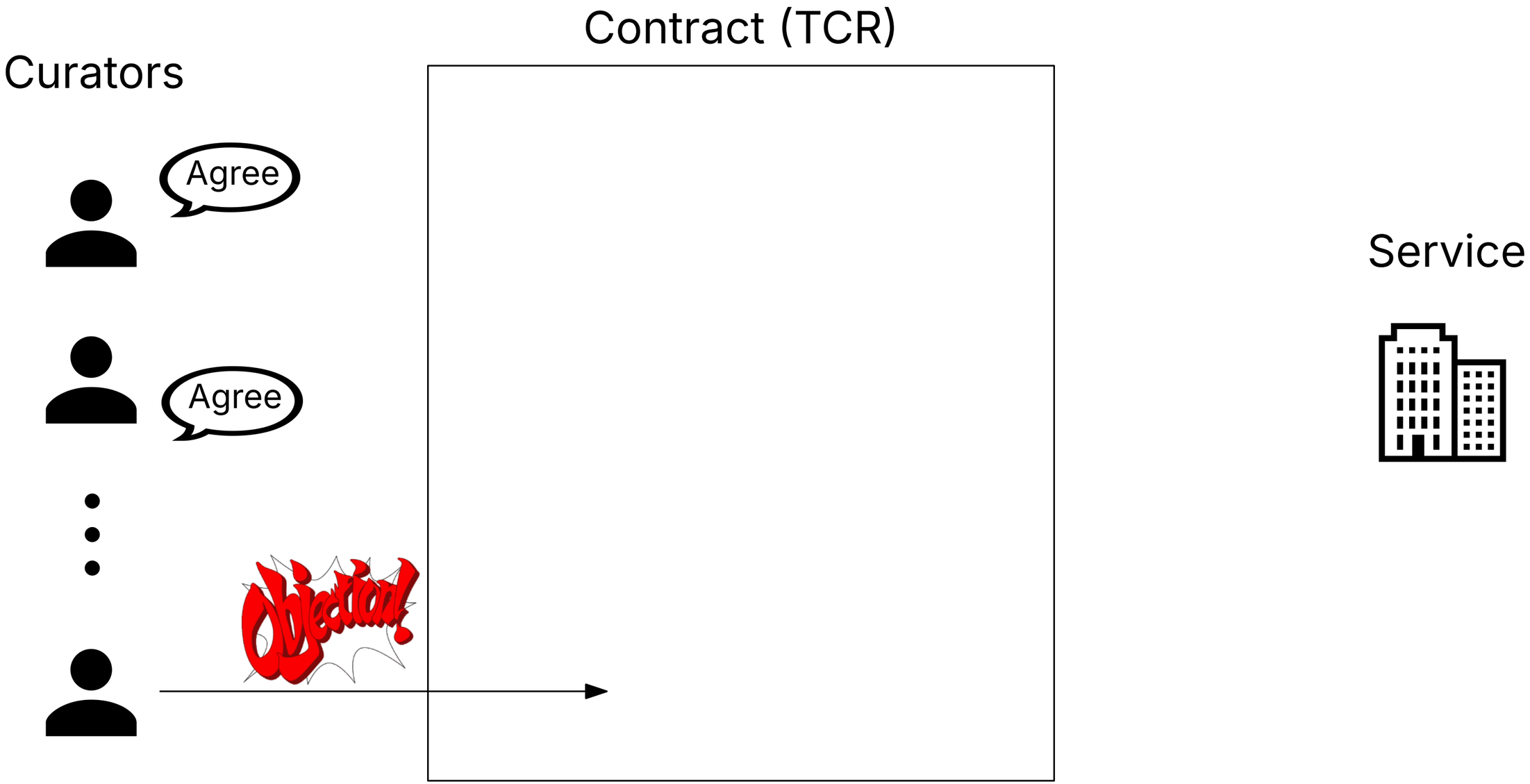
Curators

Contract (TCR)

Service

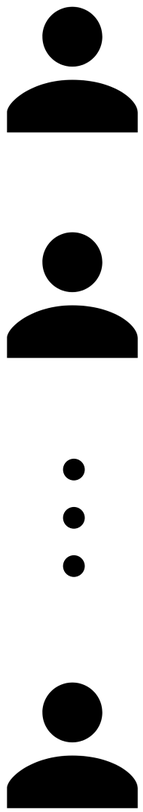


TCR Workflow



TCR Workflow

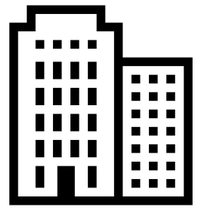
Curators



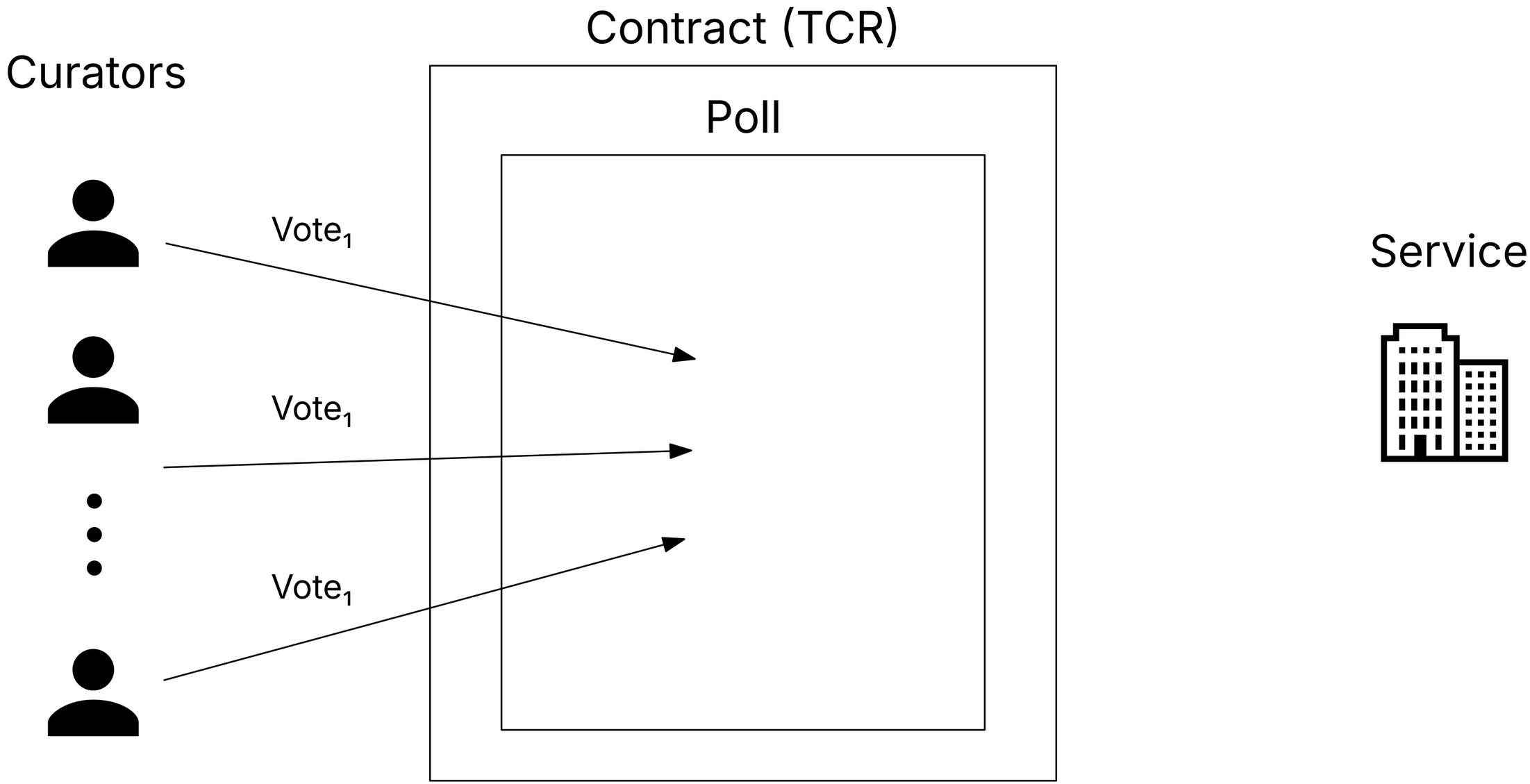
Contract (TCR)

Poll

Service

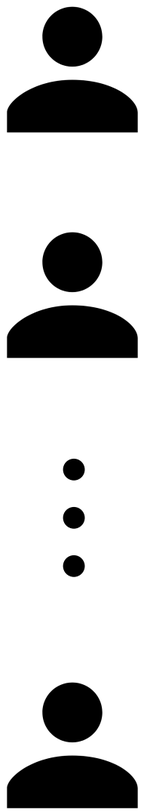


TCR Workflow



TCR Workflow

Curators

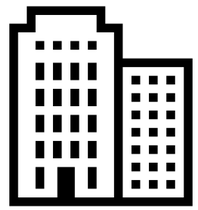


Contract (TCR)

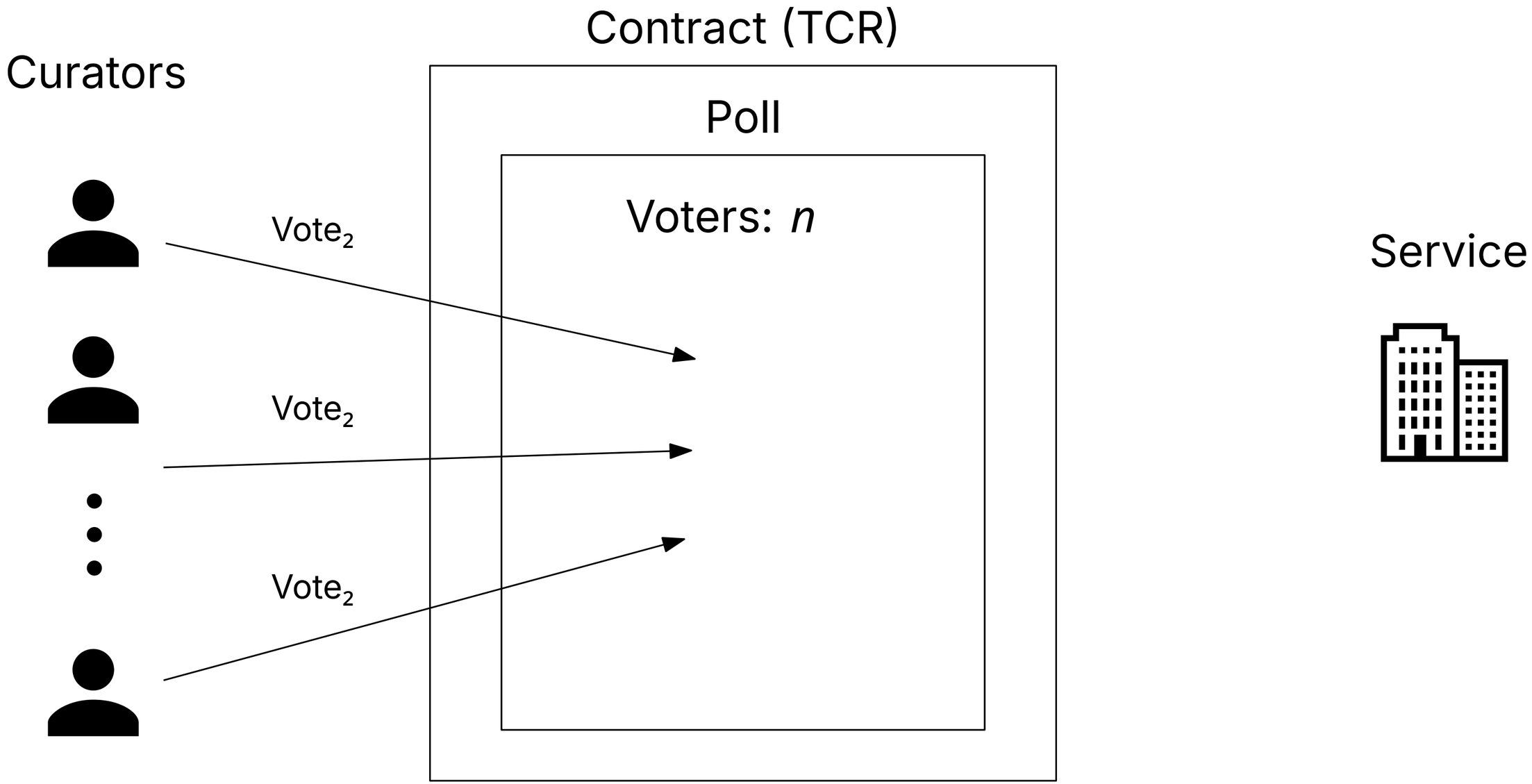
Poll

Voters: *n*

Service

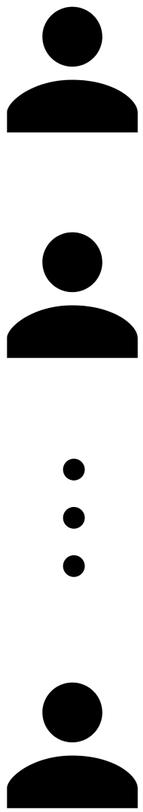


TCR Workflow



TCR Workflow

Curators



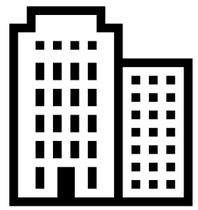
Contract (TCR)

Poll

Voters: *n*

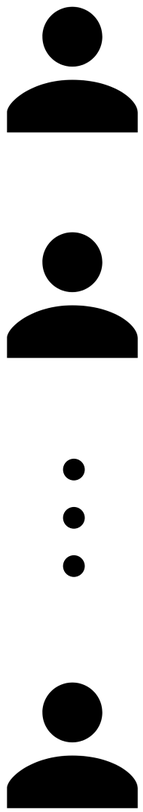
Vote1[], Vote2[]

Service



TCR Workflow

Curators



Contract (TCR)

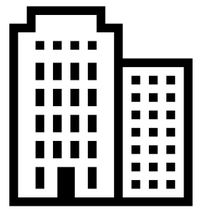
Poll

Voters: *n*

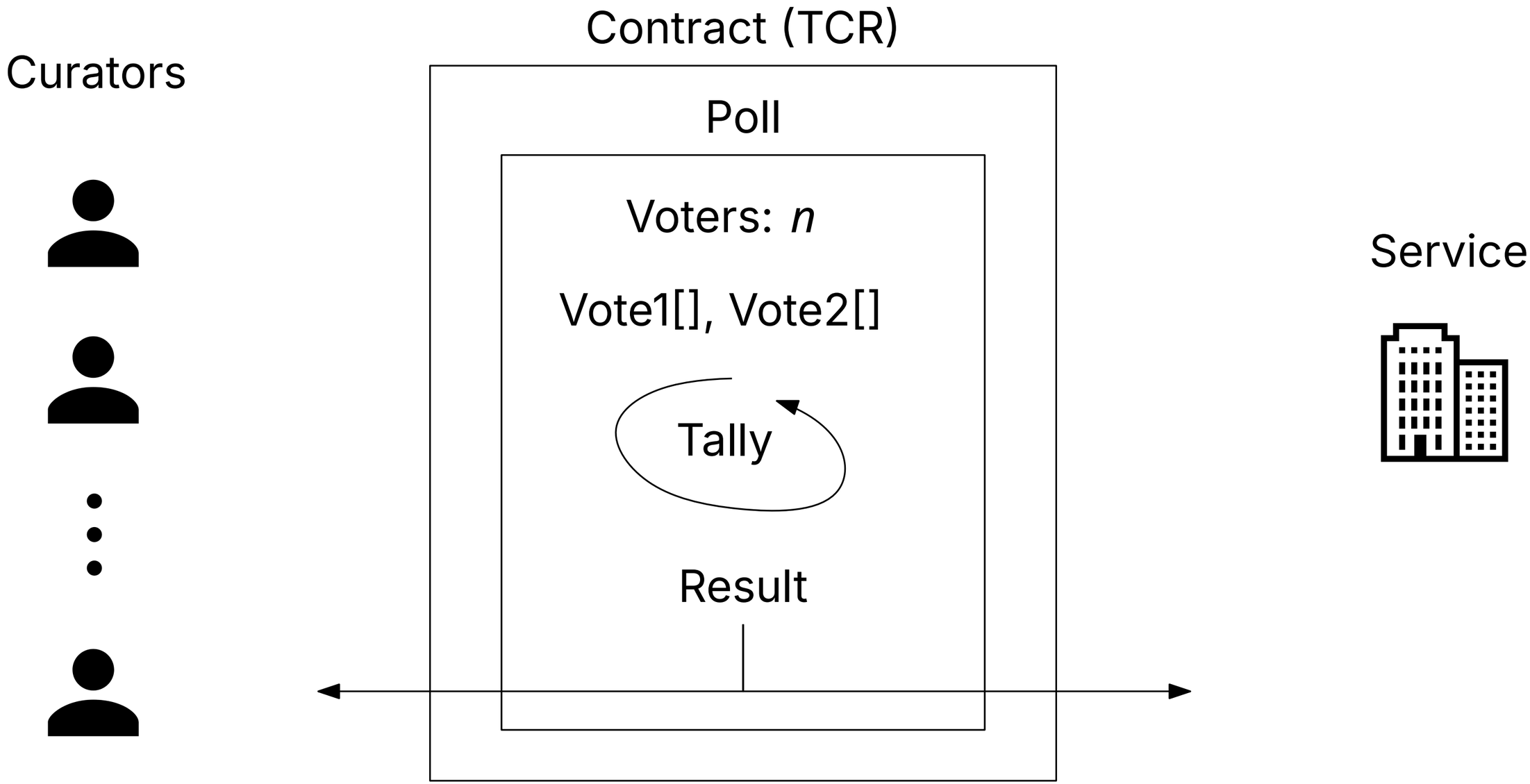
Vote1[], Vote2[]

Tally

Service



TCR Workflow



The Adversary $\mathcal{A}$

The Adversary $\mathcal{A}$

Assumptions

- PPT
- DDH and square-DDH are hard
- Can’t break non-interactive Sigma protocols

The Adversary $\mathcal{A}$

Assumptions

- PPT
- DDH and square-DDH are hard
- Can’t break non-interactive Sigma protocols

Capabilities

- Controls of malicious players
- Advises honest players
- Can see entire state of TCR

The Adversary $\mathcal{A}$

Assumptions

- PPT
- DDH and square-DDH are hard
- Can’t break non-interactive Sigma protocols

Capabilities

- Controls of malicious players
- Advises honest players
- Can see entire state of TCR

Goals

- Gain information about the vote of an honest player
- Change vote between rounds or vote other than 0 and 1

Security Guarantees

Security Guarantees

Vote secrecy: No honest player's vote can be discovered

J. D. C. Benaloh, Verifiable Secret-Ballot Elections. Yale University, 1987.

Security Guarantees

Vote secrecy: No honest player's vote can be discovered

Dispute freeness: No misbehaviour will go unnoticed

J. D. C. Benaloh, Verifiable Secret-Ballot Elections. Yale University, 1987.

Limitations

- Coercion/receipt freeness
- Performance dependent on number of voters

Conclusion

- Provably secure TCR construction
- Secret voting
- No trusted authority
- First formal approach to the subject

Questions?

Thank you!