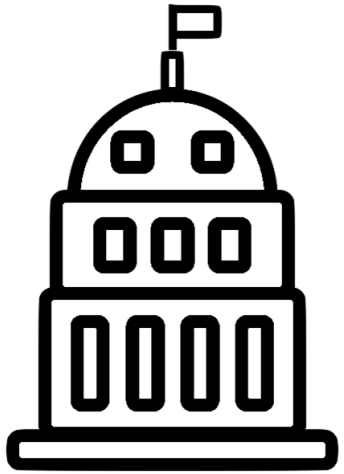
Lecture 17: Accountability

https://web3.princeton.edu/principles-of-blockchains/

Professor Pramod Viswanath
Princeton University

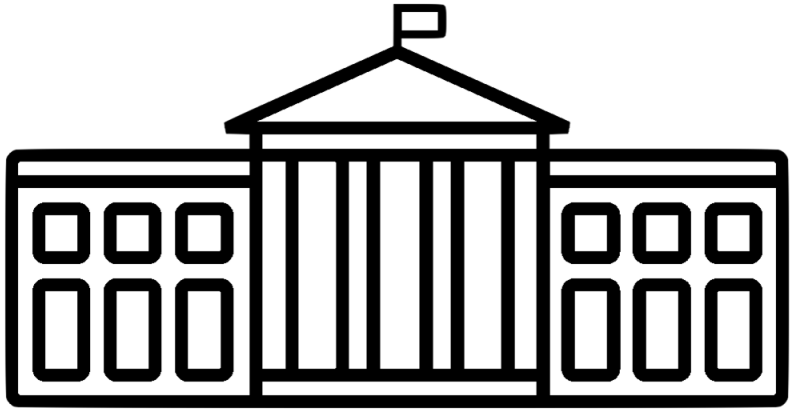
This lecture:
Accountability – malicious actors can be identified by public log;
Provides a new kind of security via “slashing”; allows “insurance”

Governance System



Legislative

Protocol description



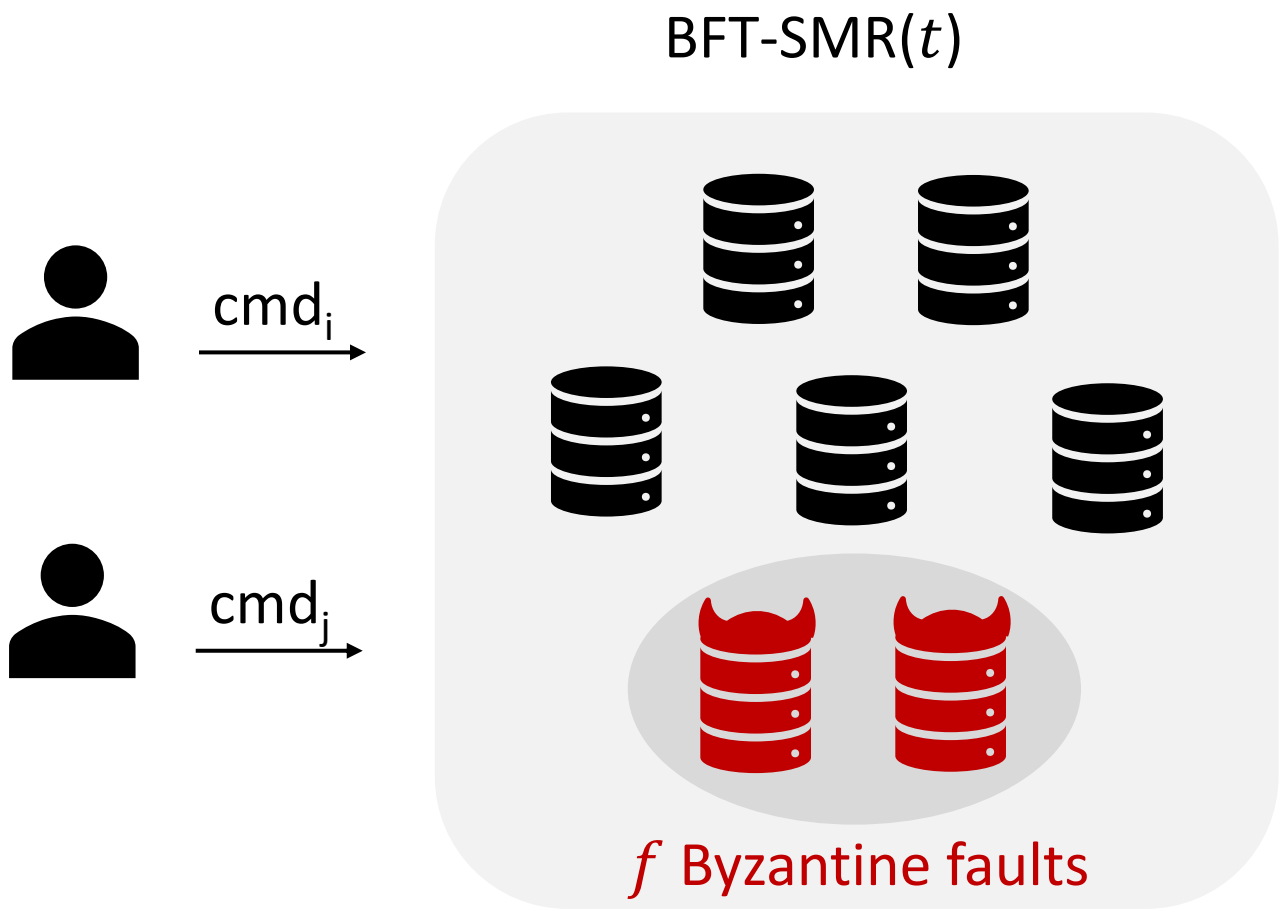
Executive

Incentives and Fees

Judicial

???

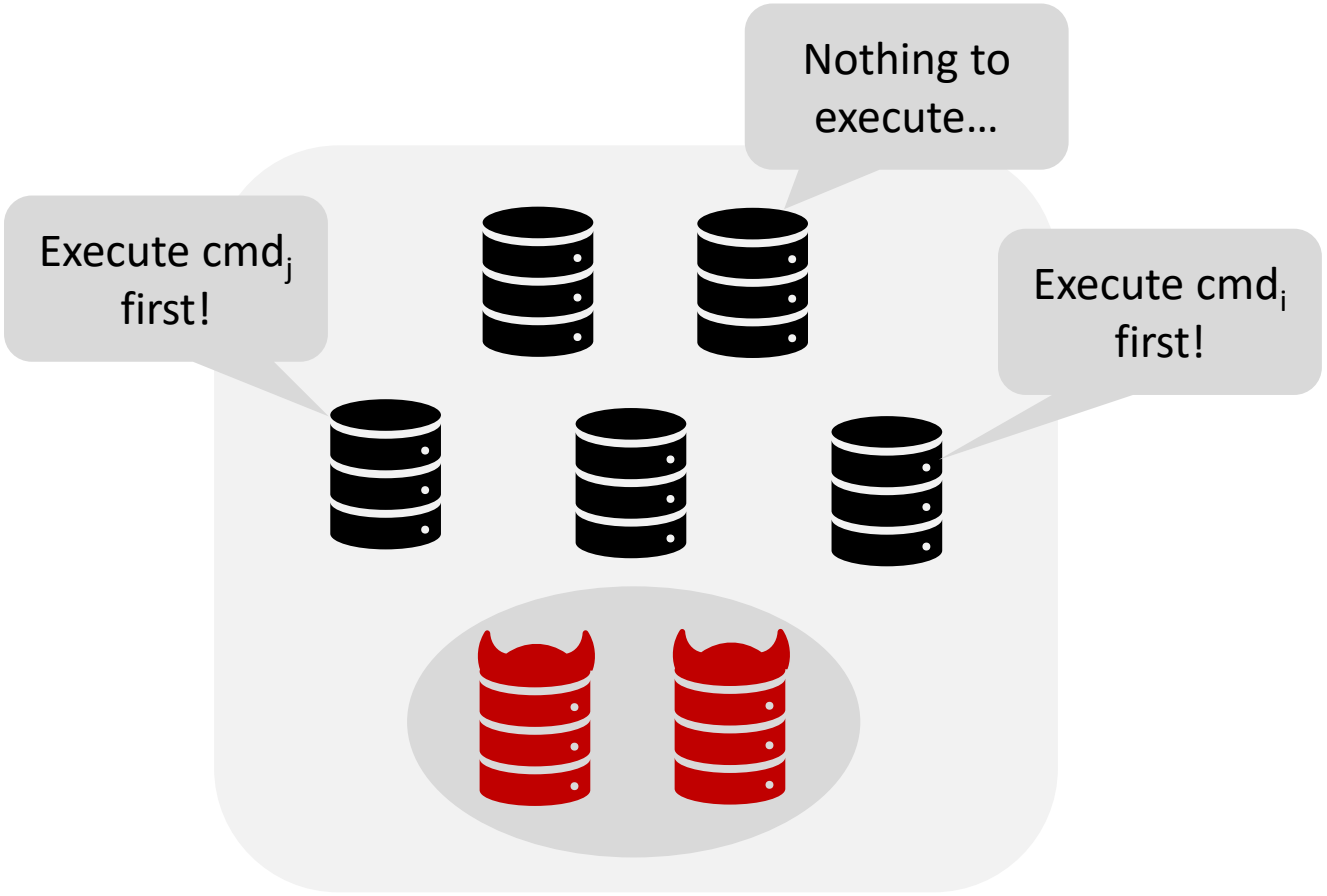
Legislative: BFT Protocols



When $f \leq t$, non-faulty parties eventually agree on the same sequence of values.

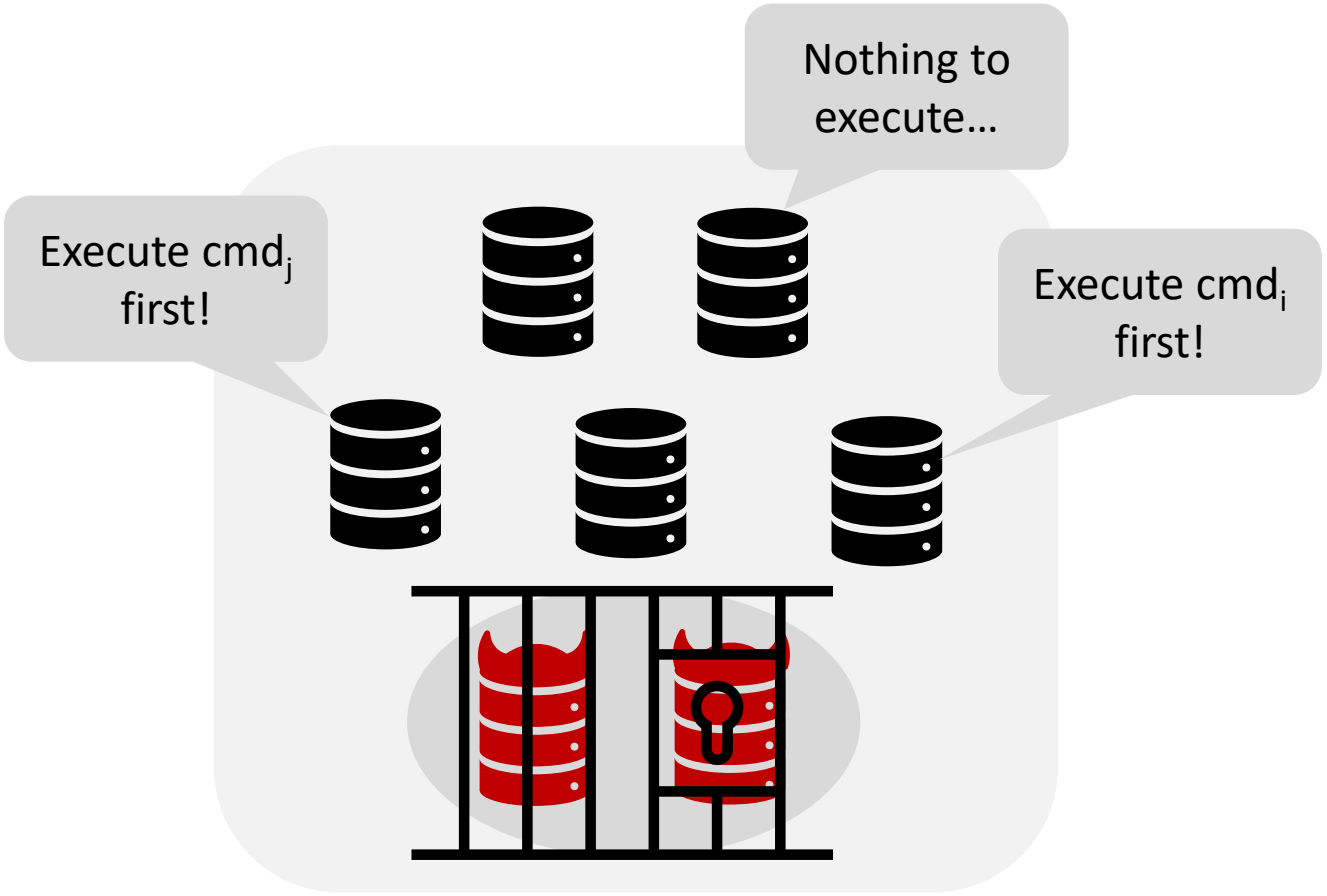
What happens when $f > t$?

BFT Protocol Forensics



Safety / liveness violation

Judicial: BFT Protocol Forensics



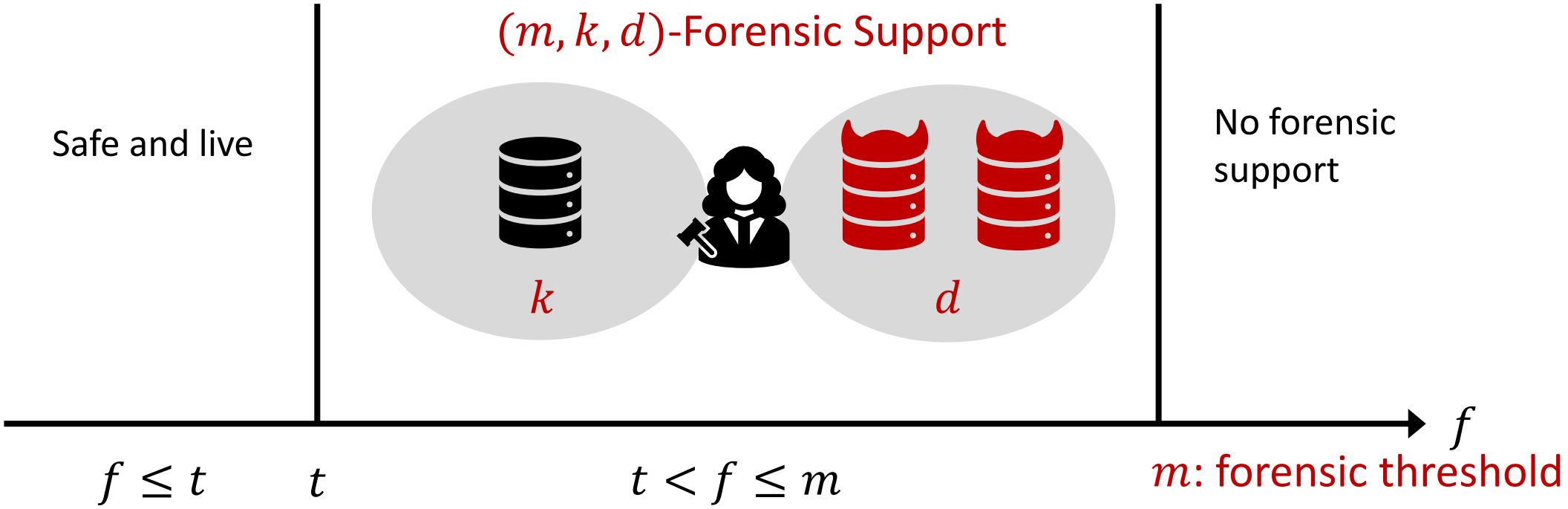
Safety / liveness violation

Forensic support: provide irrefutable evidence of bad behavior

Q1: How many bad actors?
As many as possible

Q2: How to obtain such evidence?
As distributed as possible

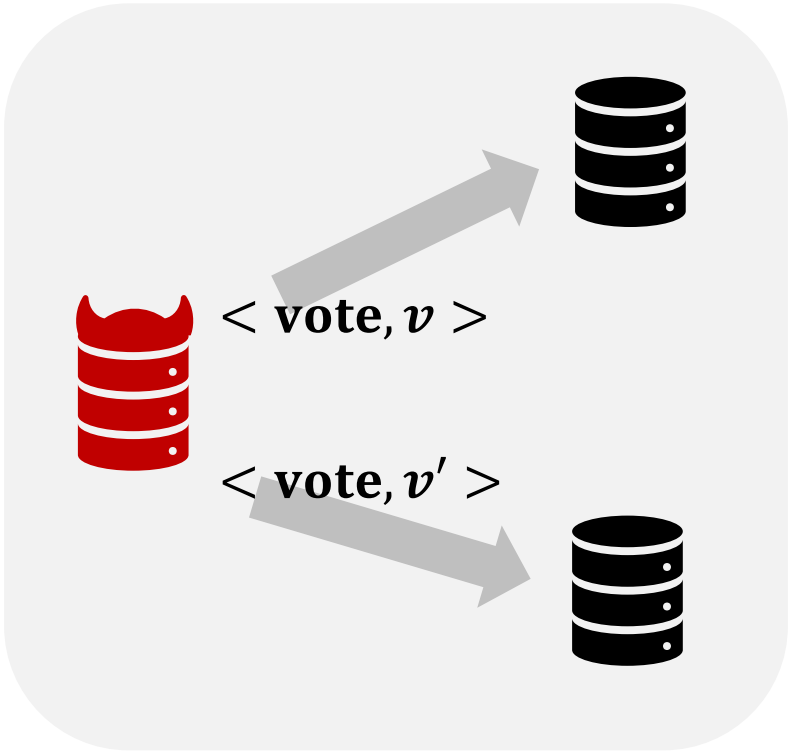
Forensic Support



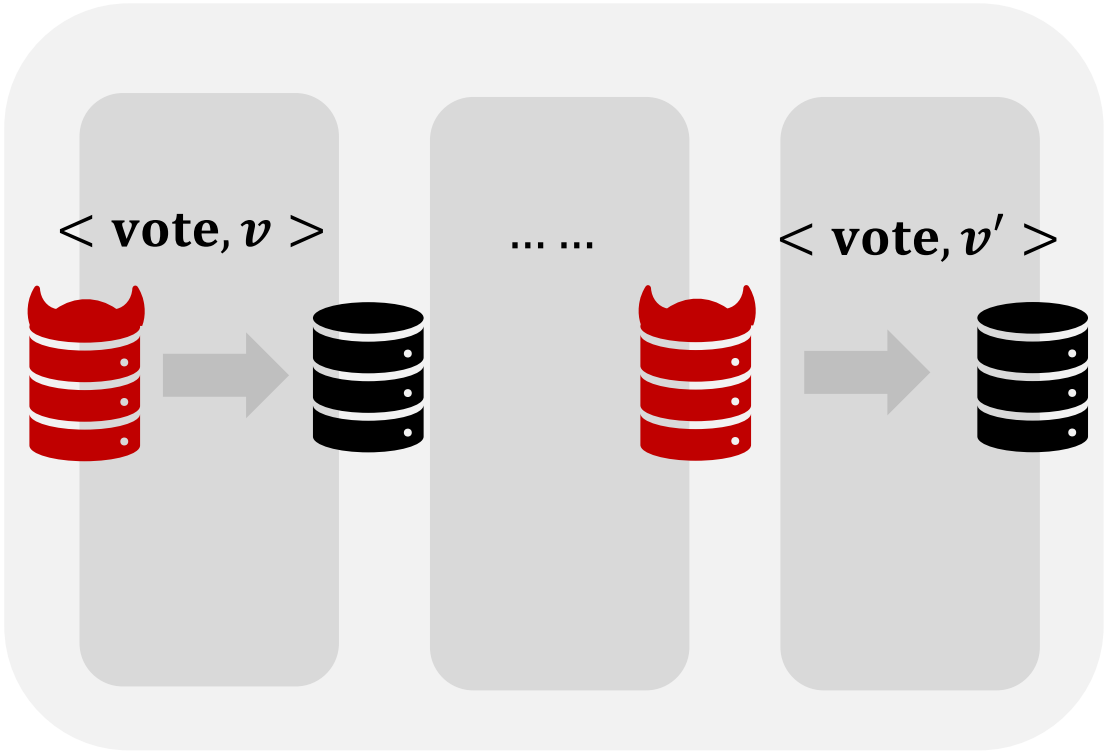
k: number of honest witnesses

d: number of Byzantine replicas detected

Intuition for Forensics

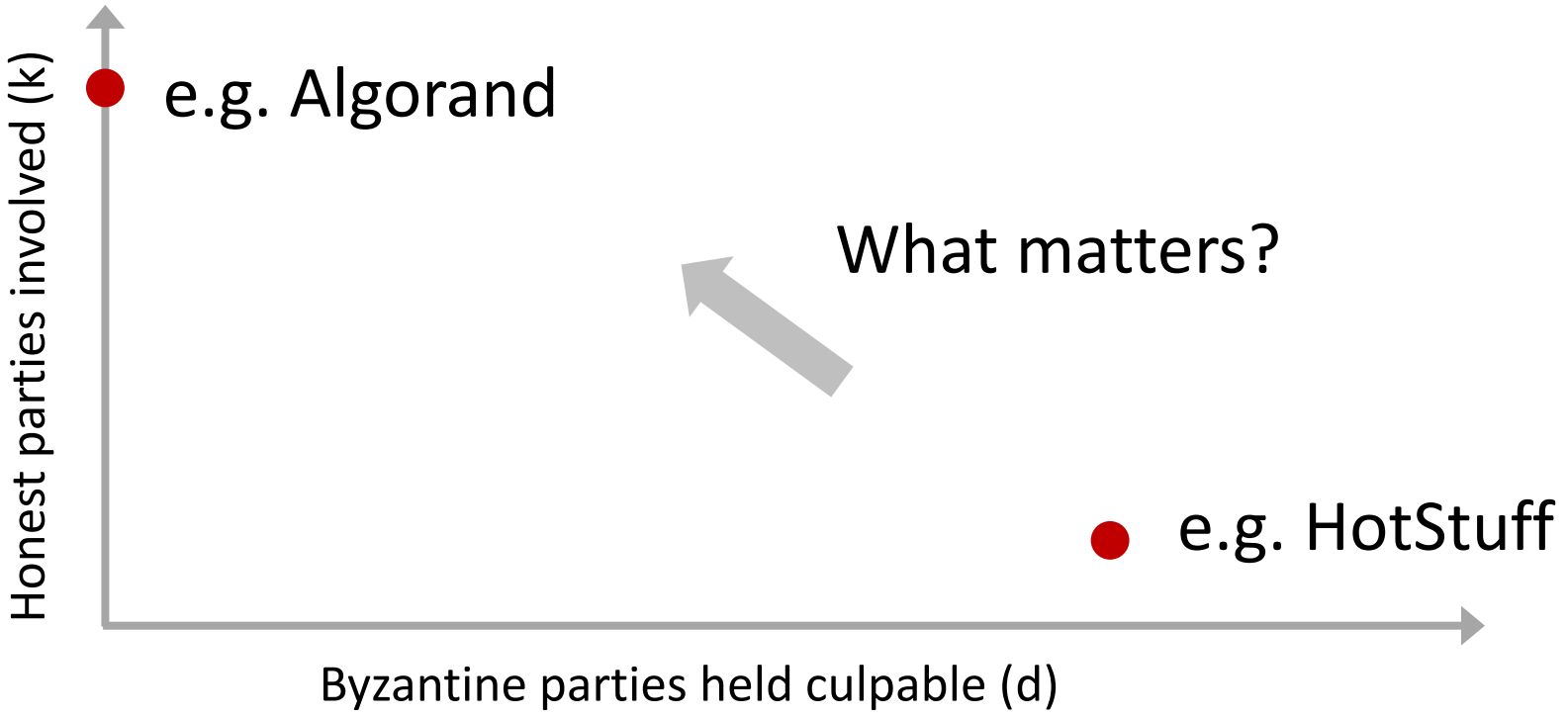


Double vote



Multi-stage protocol

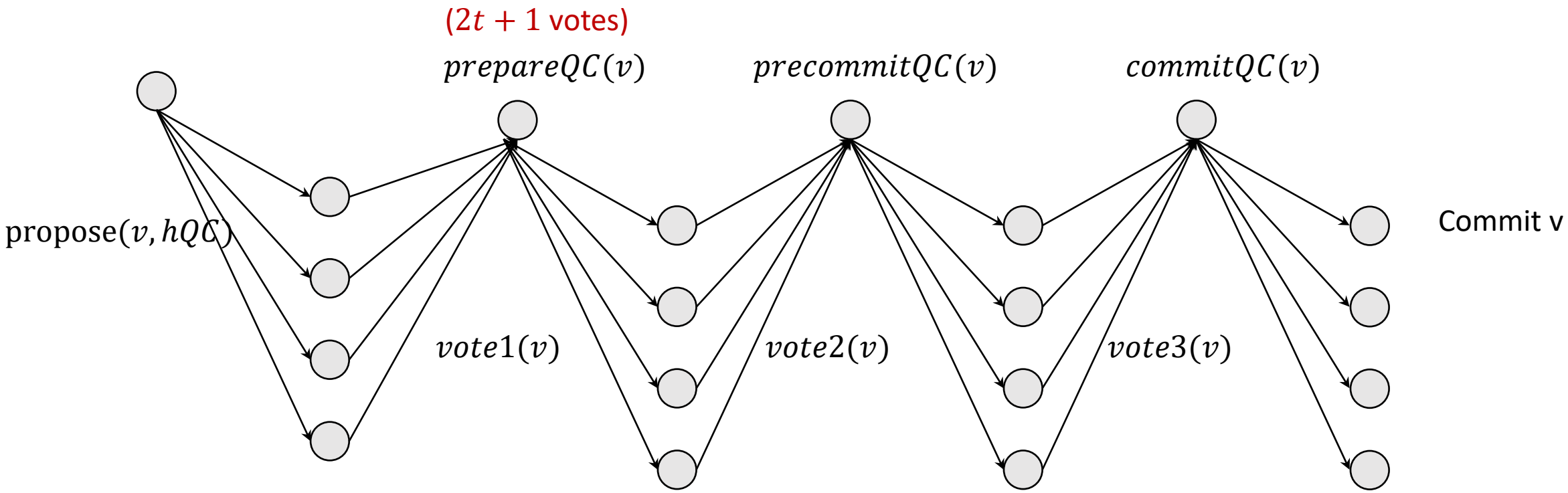
This Talk


Honest parties involved (k)
e.g. Algorand
What matters?
e.g. HotStuff
Byzantine parties held culpable (d)

Case Study: HotStuff

- Partially synchronous protocol, tolerates 1/3 Byzantine faults $(n = 3t + 1)$
- Linear communication complexity and responsiveness
- Consensus engine for multiple blockchains

Case Study: HotStuff

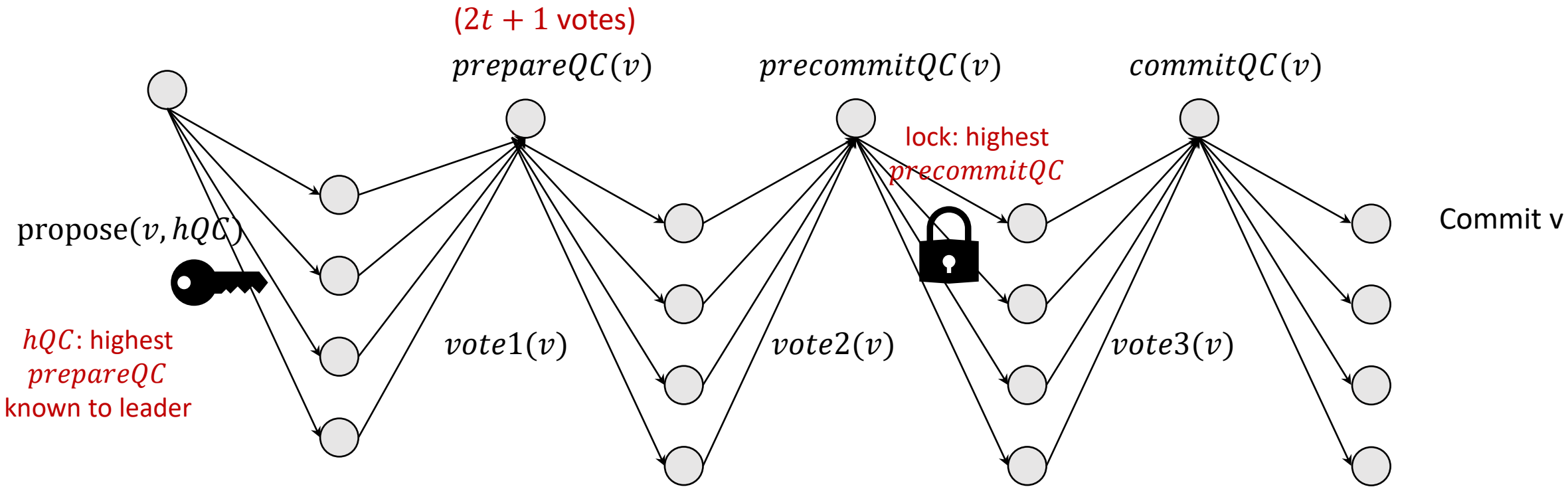


Messages in some view e

Case Study: HotStuff

Safety $(f \leq t)$ = uniqueness of QC + voting rule

A node locked on v will not vote differently unless hQC shared by leader is from a higher view



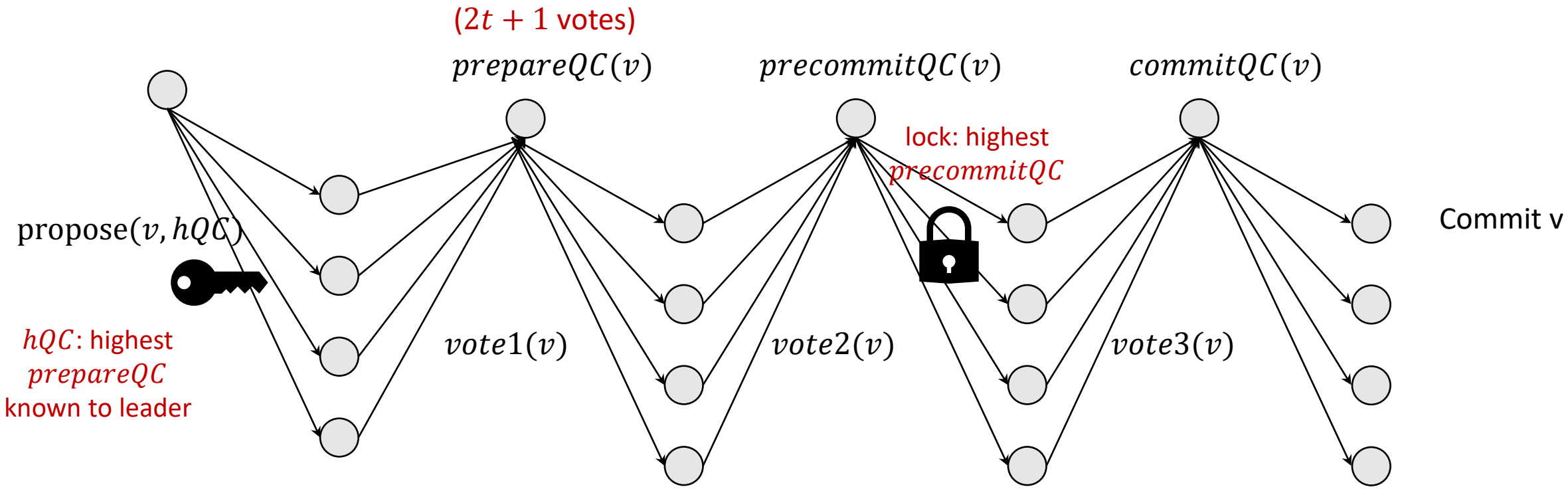
Messages in some view e

Safety Violation of HotStuff

Safety violation $(f > t)$ = ~~uniqueness~~ of QC

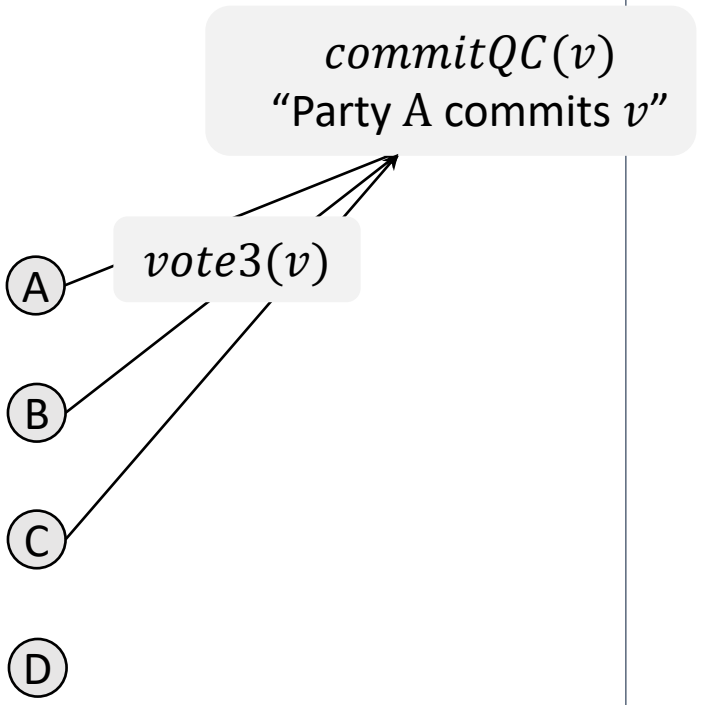
double vote

or vote for different values without hQC from a higher view



Messages in some view e

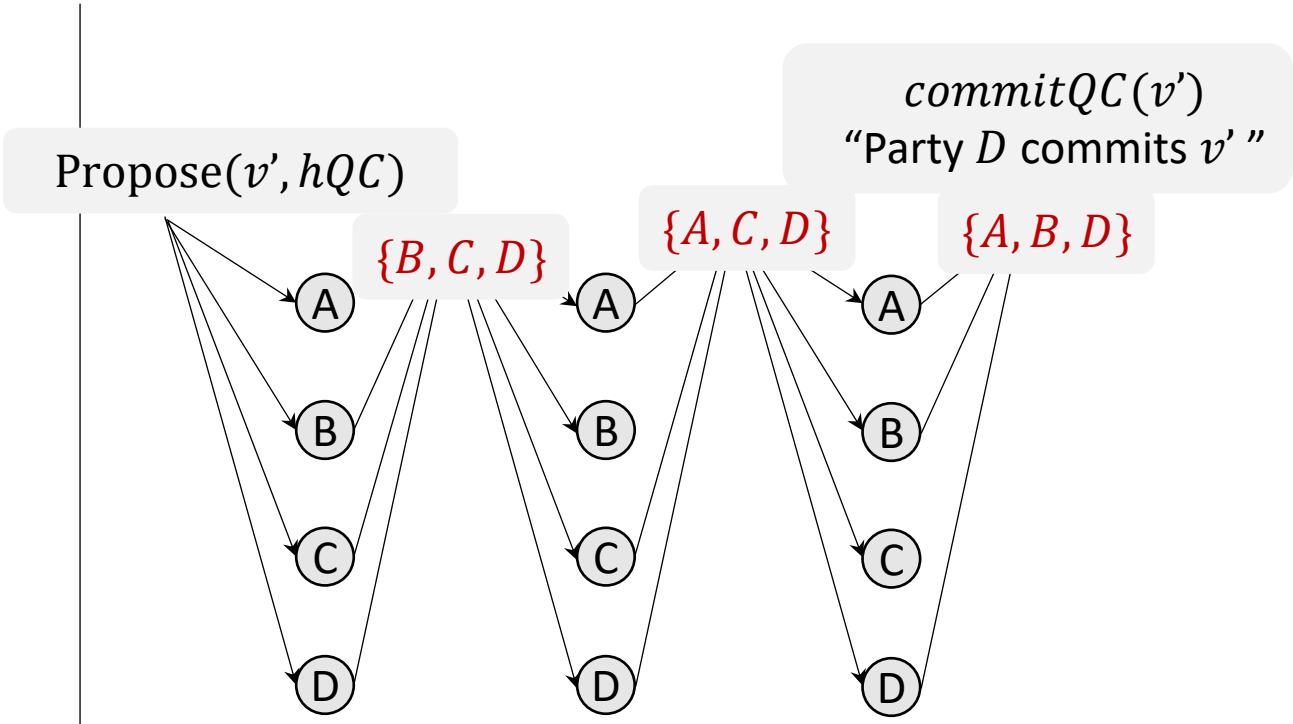
An Attack Across Views



View e

No commits in these views

. . .

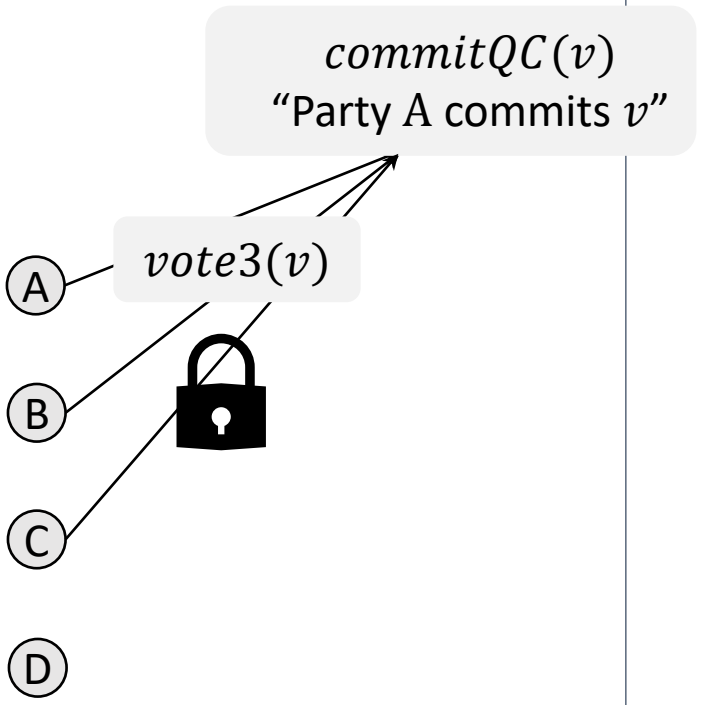


View e'

An Attack Across Views

Case1: B, C are malicious if $hQC.view \leq e$

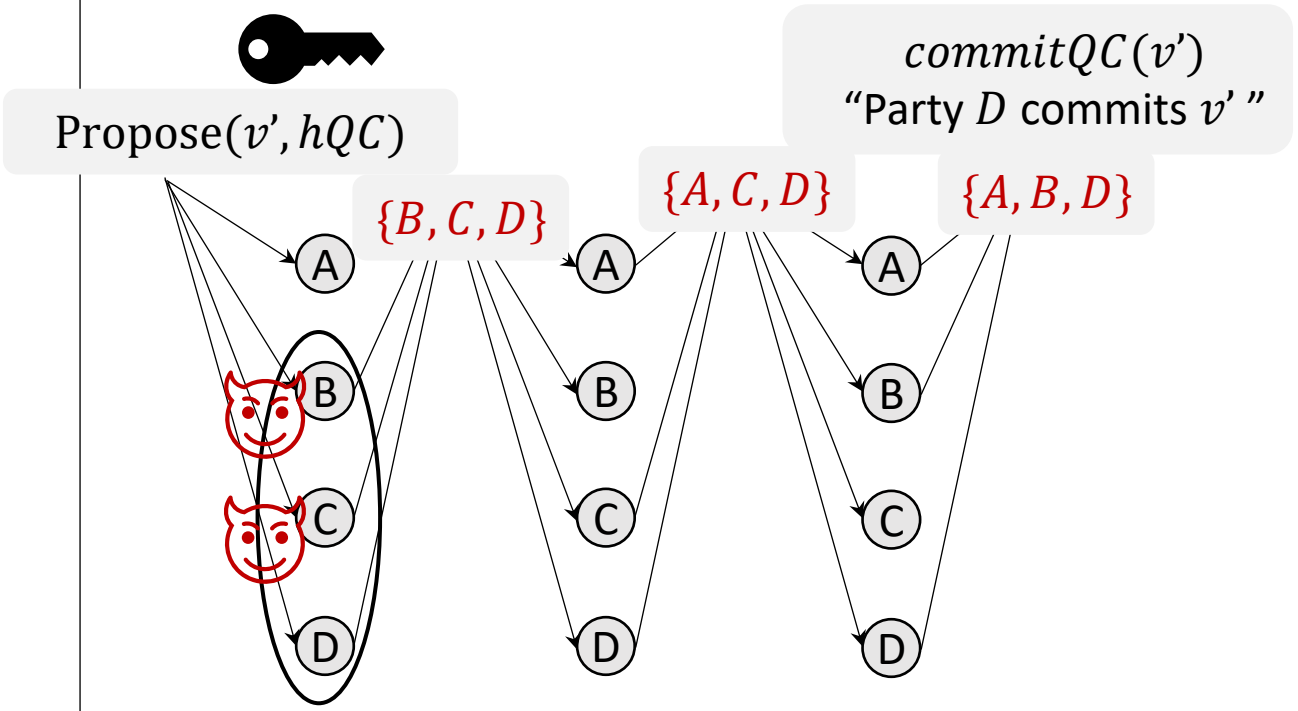
Case2: If $hQC.view > e$, look back, find a view where Case1 happens



View e

No commits in these views

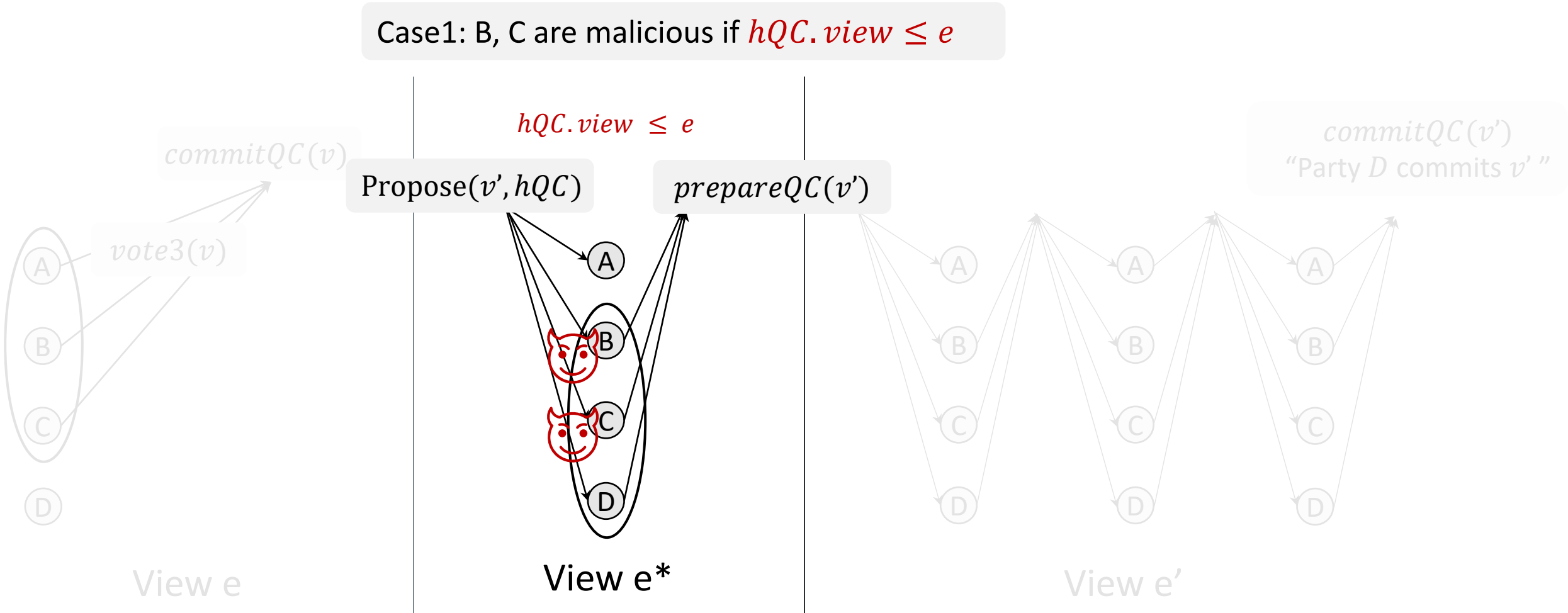
. . .



View e'

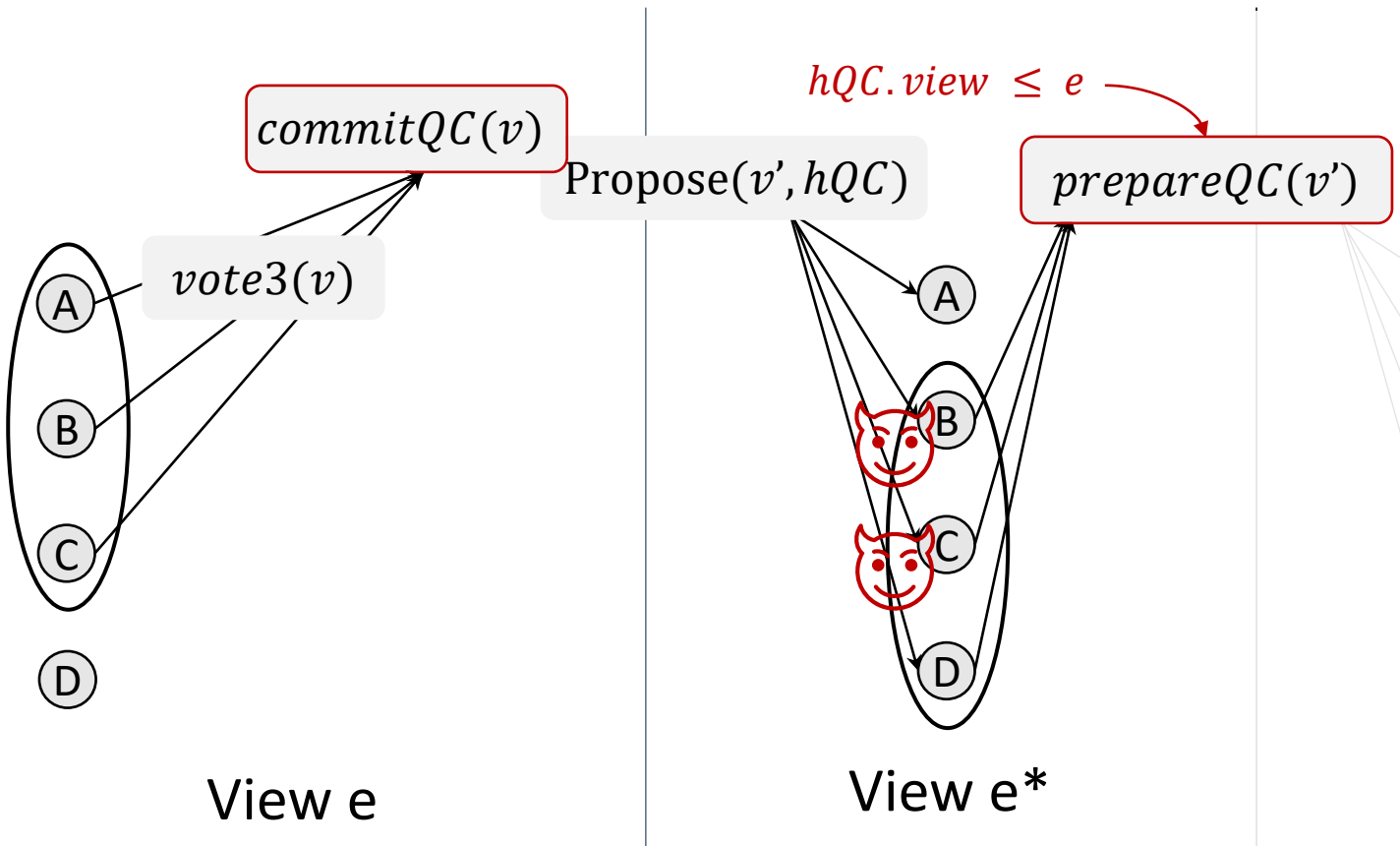
An Attack Across Views

e^*: first view $> e$, where a $prepareQC$ for a different value was formed



Forensic Support for HotStuff

$prepareQC(v') = \{< \text{vote1}, e^*, v', \boldsymbol{hQC.view} >\}_{2t+1}$



- $d = t + 1$

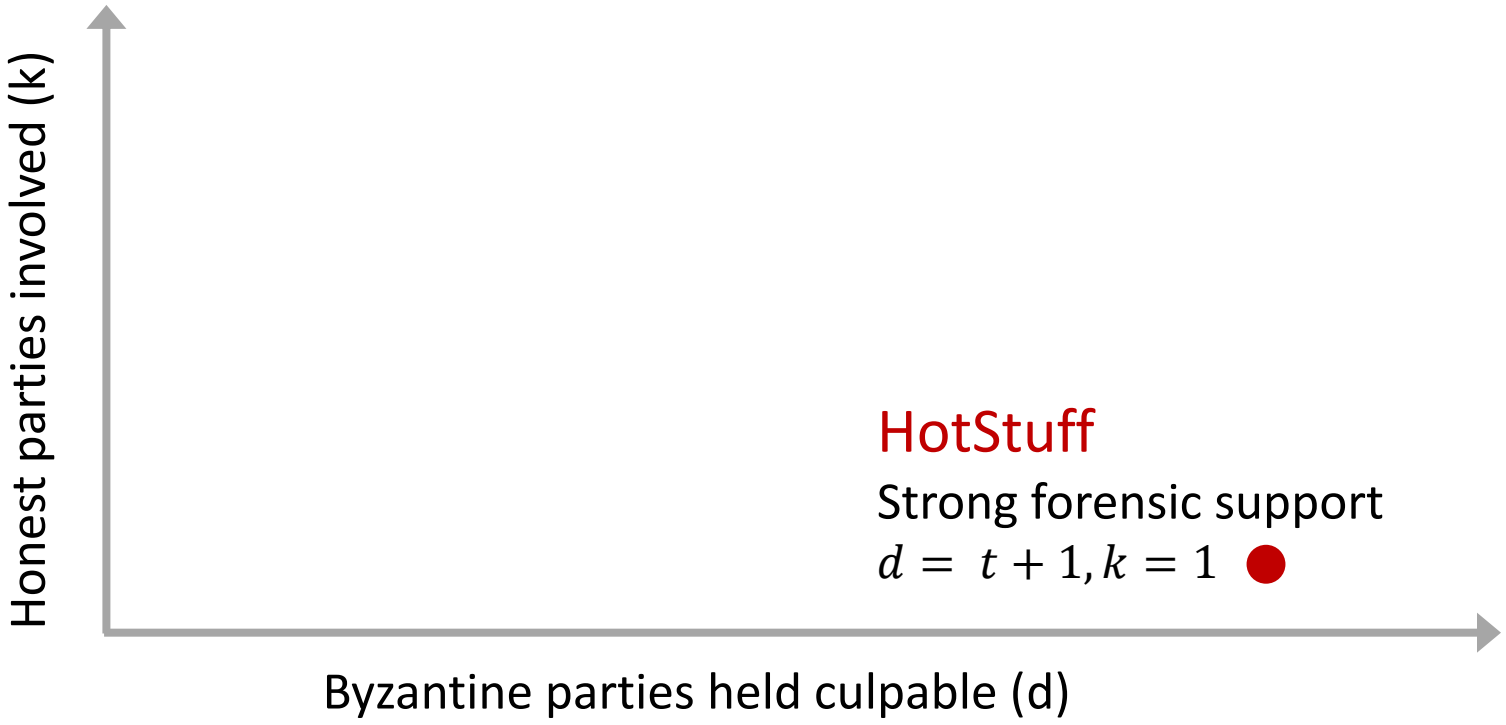
  $commitQC(v) \cap prepareQC(v')$

- $k = 1$: one node who receives $prepareQC(v')$ =

  $\{< \text{vote1}, e^*, v', hQC.view >\}_{2t+1}$

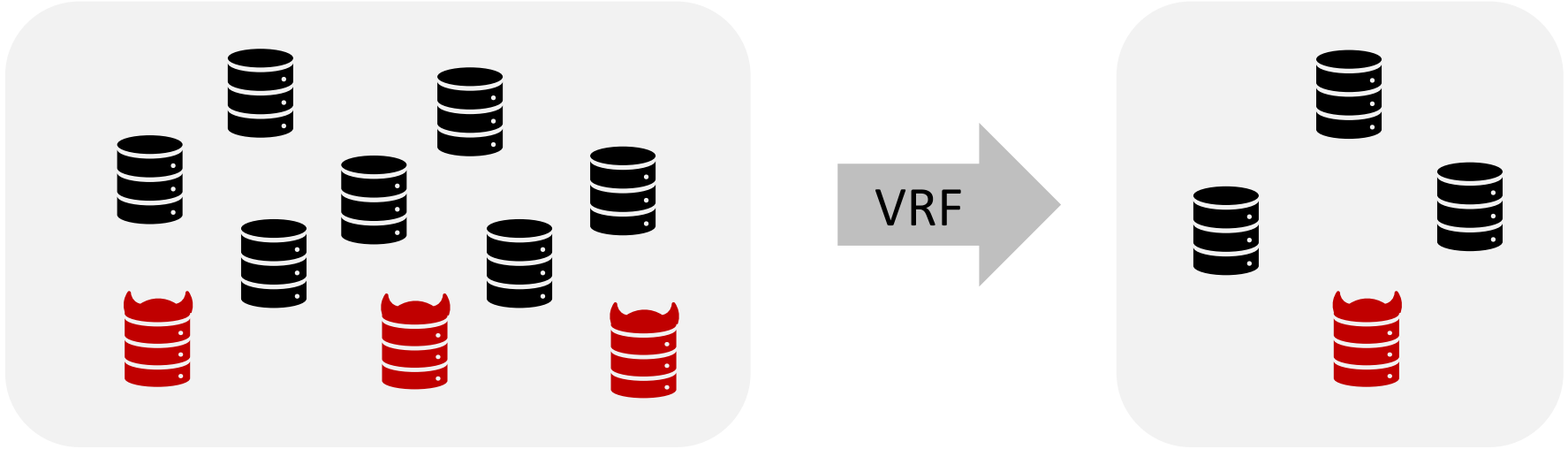
  where $hQC.view \leq e$

Strong Forensic Support



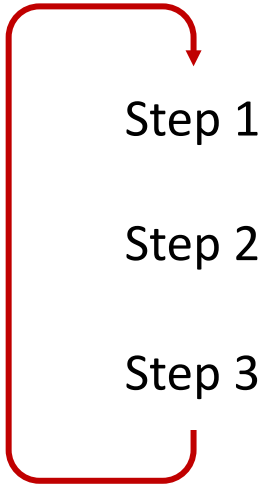
Case Study: Algorand BA

- Algorand BA: Synchronous protocol, tolerating 1/3 faults [CM'16]
- Player replaceable



Case Study: Algorand BA

- Propagate local value b
- Receive values within a synchronous step:
  - $\#(0) > 2t$, update $b = 0$ (terminate if step 1)
  - $\#(1) > 2t$, update $b = 1$ (terminate if step 2)
  - Else
    - Step 1: set $b = 0$
    - Step 2: set $b = 1$
    - Step 3: set $b =$ common coin

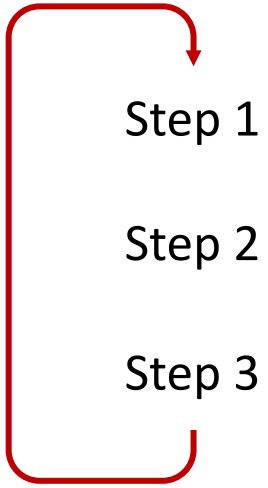


Safety intuition ($f \leq t$): Suppose a party commits $b = 0$

- All ($> 2t$) honest parties have $b = 0$
- Honest parties never change their value to $b = 1$

Safety Violation of Algorand

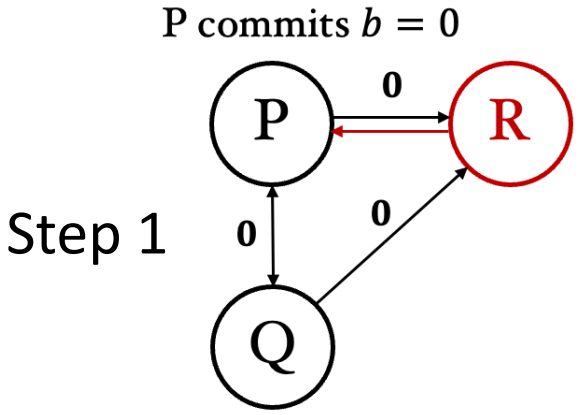
- Propagate local value b
- Receive values within a synchronous step:
  - $\#(0) > 2t$, update $b = 0$ (terminate if step 1)
  - $\#(1) > 2t$, update $b = 1$ (terminate if step 2)
  - Else
    - Step 1: set $b = 0$
    - Step 2: set $b = 1$
    - Step 3: set $b =$ common coin



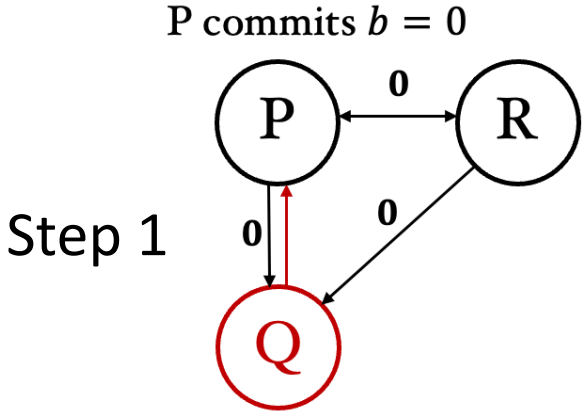
Safety intuition ($f > t$ Suppose a party commits $b = 0$

- $\leq 2t$ honest parties have $b = 0$
- Honest parties r can hange their value to $b = 1$

Attack on Algorand BA

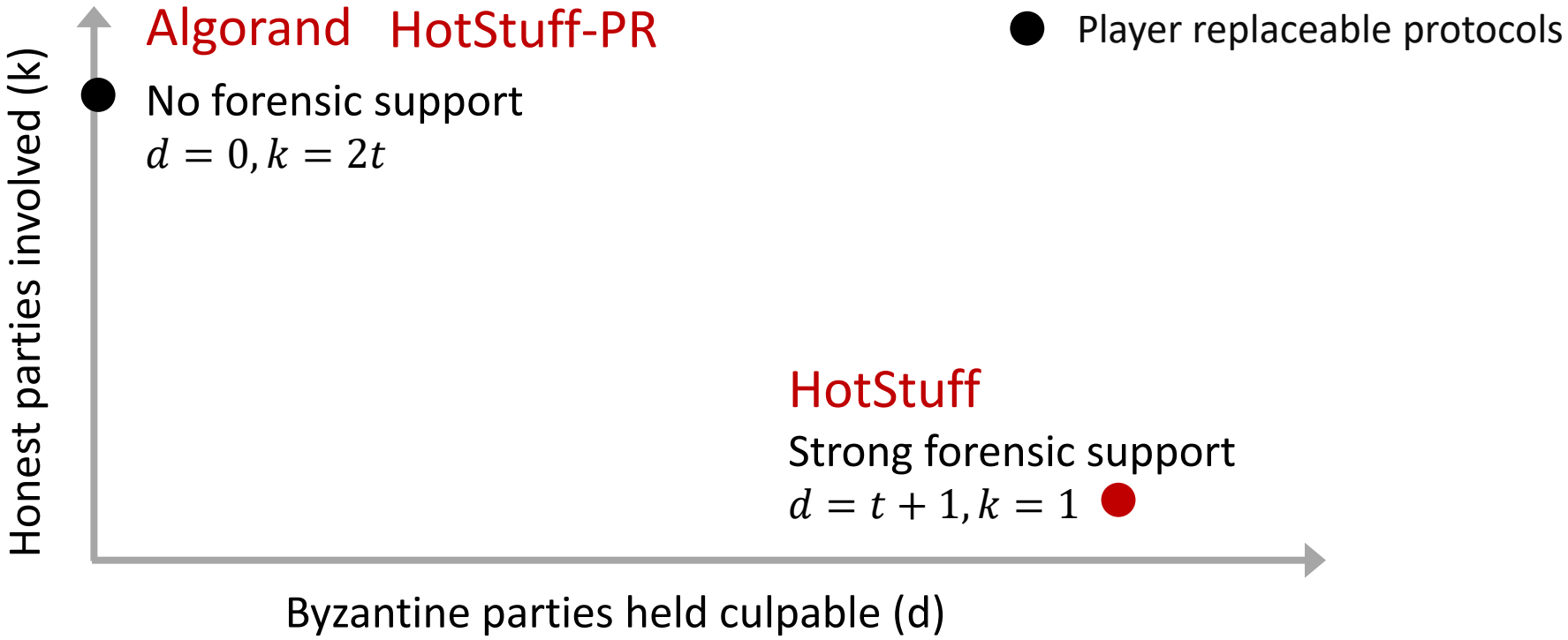


World 1: Culprits Do Not Send b



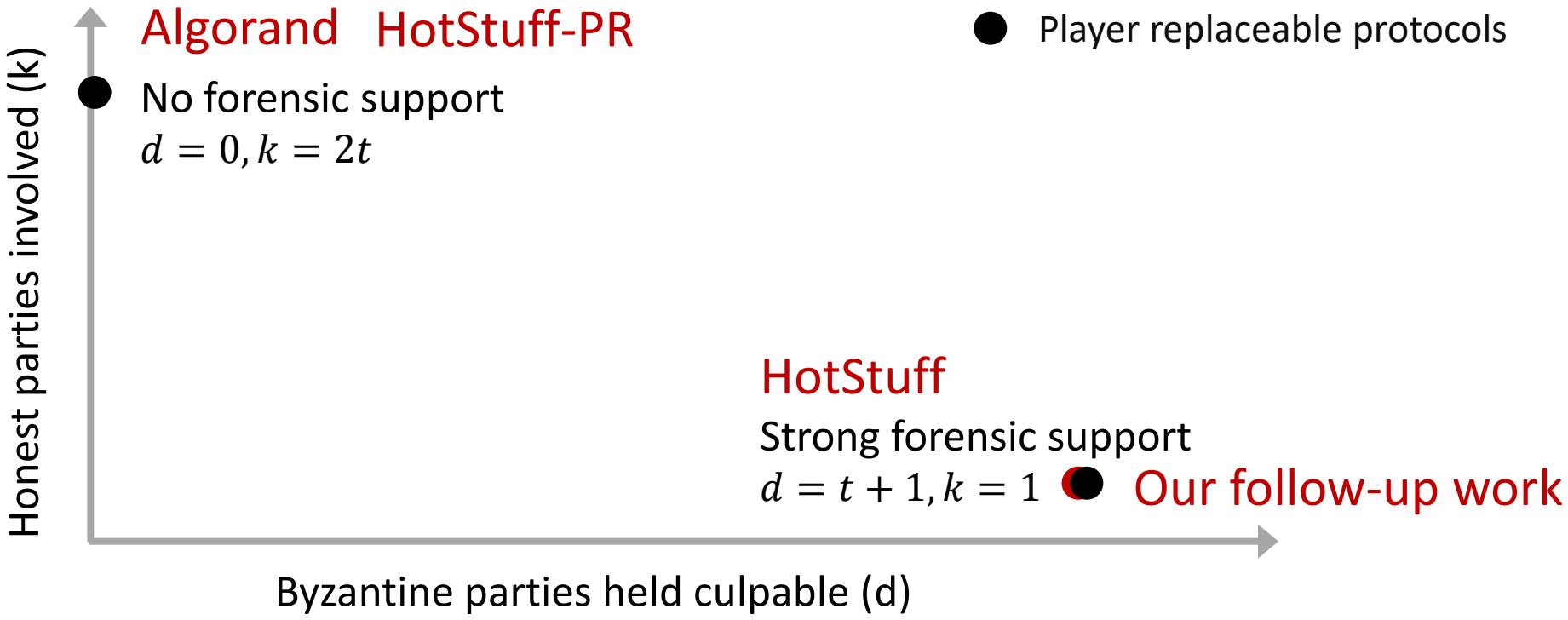
World 2: Culprits Change b

What Impairs Forensic Support?



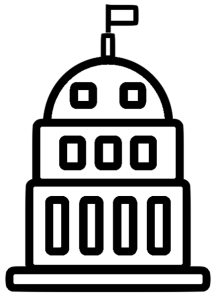
Question: Does Player replaceability mean no forensic support?

What Impairs Forensic Support?



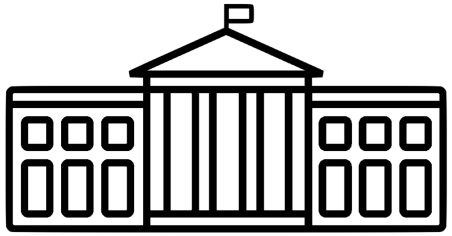
Question: Does Player replaceability mean no forensic support?

Summary



Legislative

Protocol description



Executive

Incentives

Judicial

Forensic Support

- **Protocol-level forensics**
  - Case studies
  - Protocol designs: player replaceable + strong forensic support
  - Practicality: CBDC
- **Application-level forensics**
  - NFT marketplace: wash trades
  - Anomaly detection

Summary: Accountability boosts security

- Security is one side of the coin
  - Enough participants follow protocol
- What happens if the security is broken? Forensics.
  - Allows accountability
- Slashing conditions
  - Participants put up collateral that can be “slashed” if found culpable
  - Objective “slashing conditions”
- Key distinguishing feature of PoS
  - Ethereum 2.0; 32 ETH staked by each participant

Attendance : NFT Drop

https://poap.website/well-style-individual

- Mint token to Metamask.
- Submit tx hash for attendance claim.

- Instructions in Ed pinned posts.