# Towards Rational Consensus in Honest Majority

Varul Srivastava, Sujit Gujar
Machine Learning Lab, IIIT Hyderabad

February 9, 2025

# Introduction & Motivation

**Problem Statement:**

- Achieving distributed consensus under different threat models.
- Rational Fault Tolerance (RFT) is underexplored for Atomic Broadcast (ABC).

# Introduction & Motivation

**Problem Statement:**

- Achieving distributed consensus under different threat models.
- Rational Fault Tolerance (RFT) is underexplored for Atomic Broadcast (ABC).

**Why This Matters:**

- Critical for blockchain security and decentralized systems.
- Existing approaches (CFT, BFT) do not handle rational adversaries well.

# Background & Key Concepts

- **Consensus Types:**
  - Byzantine Agreement (BA)
  - Atomic Broadcast (ABC)
  - Rational Consensus (RC)

# Background & Key Concepts

- **Consensus Types:**
  - Byzantine Agreement (BA)
  - Atomic Broadcast (ABC)
  - Rational Consensus (RC)
- **Threat Models:**
  - Crash Fault Tolerance (CFT)
  - Byzantine Fault Tolerance (BFT)
  - Rational Fault Tolerance (RFT)

# Our Contributions

- Show impossibility of ABC under certain rational threat models.
- Identify a security flaw in the TRAP protocol (alternative Nash Equilibrium leads to disagreement).
- Introduce **pRFT**, a novel protocol achieving Rational Consensus under RFT with accountability.

# Player Types & Impossibility Results

**Types of Rational Players:**

- $\theta = 3$: Prefer liveness, censorship, or forking attacks $\Rightarrow$ No ABC possible.
- $\theta = 2$: Prefer censorship or forking $\Rightarrow$ No ABC possible.
- $\theta = 1$: Prefer only forking $\Rightarrow$ Can design a solution.

# Weakness of TRAP Protocol

- TRAP protocol uses baiting-based strategies to deter rational players from deviation.
- Issue: There exists a **more attractive Nash Equilibrium** that leads to disagreement.

# Weakness of TRAP Protocol

- TRAP protocol uses baiting-based strategies to deter rational players from deviation.
- Issue: There exists a **more attractive Nash Equilibrium** that leads to disagreement.

**Example Game with Two Nash Equilibria:**

| | $a$ | $b$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $A$ | (1,1,1) | (1,1,0) | (1,0,1) | (-2,2,2) |
| $B$ | (0,1,1) | (1,-2,1) | (2,2,-2) | (0,0,0) |

# Comparison with Existing Protocols

| Protocol | Msg Complexity | Acc. | Threat Model |
|---|---|---|---|
| pBFT (CL99) | $O(n^3)$ | $\times$ | $t < \frac{n}{3}$ |
| HotStuff (YIN19) | $O(n^2)$ | $\times$ | $t < \frac{n}{3}$ |
| Polygraph (CIV21) | $O(n^3)$ | $\checkmark$ | $t < \frac{n}{3}$ |
| **pRFT (Our Work)** | $O(n^3)$ | $\checkmark$ | $t + k < \frac{n}{2}, t < k$ |

# Our Solution – pRFT Protocol

- **Key Idea:** Remove reliance on baiting by introducing **accountability**.
- **How It Works:**
  - Players deposit collateral, which is penalized if they deviate.
  - Honest players track deviations using Proof-of-Fraud (PoF).

# pRFT Protocol

**pRFT**($\overline{p}_{i=1}^{n}, t_0$)

**Propose Phase:**
**if** $i = r \bmod n$ **then**
  $\mathsf{Block}_r := \mathsf{ConstructBlock}(\overline{tx}, r, b_{parent}, p_i)$
  $h_l := \mathsf{Hash}(\mathsf{Block}_r)$
  $\mathsf{Broadcast}(\langle Propose, Block_r, h_l, r\rangle_i, s_i^{pro})$
**else**
  On Recv. $(\langle Propose, Block_r, h_l, r\rangle, s_l^{pro})$:
    $\mathsf{Broadcast}(\langle Vote, h_l, s_l^{pro}, r\rangle_i, s_i^{vote})$
**end if**

**Vote Phase:**
On Recv. $(\langle Vote, h_j, s_l^{pro}, r\rangle, s_j^{vote})$:
  $votes[h_j] := votes[h_j] \cup \{s_j^{vote}\}$
**if** for some $h_*, vote[h_*].size \geq n - t_0$ **then**
  $\mathsf{Broadcast}$
  $(\langle Commit, h_*, s_l^{pro}, vote[h_*], r\rangle_i, s_i^{com})$
**end if**

**Commit Phase:**
On Recv. $(\langle Commit, h_j, s_l^{pro}, \overline{vote}_j, r\rangle, s_j^{com})$:
  $commit[h_j] := commit[h_j] \cup \{s_j^{com}\}$
**if** for some $h_*, commit[h_*].size \geq n - t_0$ **then**
  $\mathsf{Broadcast}(\langle Reveal, h_*, s_l^{pro}, commit[h_*], r\rangle_i, s_i^{rev})$
**end if**

**Reveal Phase:**
$D_i := \emptyset, M_i := \emptyset, F_i := \emptyset$
On Recv. $(\langle Reveal, h_j, s_l^{pro}, \overline{commit}_j, r\rangle, s_j^{rev})$:
  $M_i \leftarrow M_i \cup \{\overline{commit}_j\}$
  $D_i := \mathsf{ContructPoF}(M_i)$
On Recv $(\langle Final, B_j, s_l^{pro}\rangle_j, s_j)$
  $F_i \leftarrow F_i \cup \{s_j^{fin}\}$
On Recv $(\langle Expose, D_j, r\rangle, s_j)$
  $\mathsf{Stash}(D_j), r := r + 1$
**if** $|D_i| > t_0$ **then**
  $\mathsf{Broadcast}(\langle Expose, D_i, r\rangle_i, s_i^{expose})$
**else if** $|M_i| \geq n - t_0$ **then**
  $\mathsf{Broadcast}(\langle Final, B_l, s_l^{pro}\rangle_i, s_i^{fin})$
**else if** $|F_i| > \frac{n}{2}$ **then**
  $\mathsf{Broadcast}(\langle Final, B_l, s_l^{pro}\rangle_i, s_i^{fin})$
**end if**

Figure: pRFT Protocol

# Theoretical Guarantees & Security

- **Correctness:** Agreement under rational adversaries ($\theta = 1$).
- **Security:** Achieves **Dominant Strategy Equilibrium (DSE)**.
- **Efficiency:** Message complexity comparable to state-of-the-art.

# Conclusion & Future Work

- **Summary:**
  - ABC is impossible when rational players profit from attacks.
  - TRAP is insecure due to an alternative Nash Equilibrium.
  - **pRFT** achieves Rational Consensus in RFT settings.
- **Open Problems:**
  - Extending pRFT to handle more general rational player types.
  - Reducing message complexity using cryptographic techniques.

# Q&A

- Questions?

# Q&A

- Questions?
- **Idea:** Generalize the concept of focal equilibria for security of cryptographic protocols.