Towards Rational Consensus in Honest Majority

Varul Srivastava
International Institute of Information Technology
Hyderabad, India
varul.srivastava@research.iiit.ac.in

Sujit Gujar
International Institute of Information Technology
Hyderabad, India
sujit.gujar@iiit.ac.in

***Abstract*—Rational Consensus (RC) is a more realistic modelling of the traditional Byzantine Consensus problem, motivated by the recent works in Rational Cryptography. RC is the problem of achieving consensus in the presence of Rational, Byzantine and Honest players (players– participants in the consensus protocol) in a distributed system. This work focuses on consensus in multiple rounds with additional agreement on ordering among rounds which is a more general problem called Atomic BroadCast (ABC). Blockchains is an example of application of ABC.**

This work abstracts rational players in three types on their incentive structure. We show the impossibility of achieving consensus for two out of the three types of rational players under some conditions. For the third type of rational players, existing work models a single round of agreement and, therefore, doesn't capture the existence of another insecure equilibrium strategy for rational players. We finally fill the gap in the literature of a Rational ABC by proposing a novel protocol for rational consensus, namely pRFT. We prove (i) the correctness of the protocol and (ii) the communication complexity of pRFT, which is a form of *accountable* protocol, equals the best-known accountable agreement protocols.

***Index Terms*—Distributed System, Rational Consensus, Blockchains**

I. Introduction

Distributed Consensus is when multiple players with some input value participate in an agreement protocol to decide on a common value. There has been extensive work in agreement and consensus under different threat models, namely (i) Crash Fault Tolerant — where some fraction f of n players can crash (not send messages) (ii) Byzantine Fault Tolerant — where some fraction f of n players can act arbitrarily different from the protocol and (iii) Rational Fault Tolerant — where some fraction t behave like byzantine players and another fraction k are *rational* players i.e. deviating only when doing so is incentivized. Current results on each threat model are specified in Table I, placing our contribution in blue.

Ranchal-Pedrosa and Gramoli [1] introduced a general rational threat model where t byzantine players and k rational players can collude. This is called a rational threat model – $RFT(k,t)$ and the agreement problem called *Rational Consensus* (RC). The authors propose RC using *baiting based protocol* – TRAP by showing the existence of a Nash Equilibrium (NE) that achieves consensus for $t < n/3$ and $k + t < n/2$. Protocols are called *Nash Incentive Compatible* (NIC) when the honest strategy is NE. However, we show the existence of another (more preferred) NE strategy that causes disagreement for TRAP when used to solve Atomic Broadcast (ABC). The rational players may prefer this dystopic equilibrium point over the more improbable secure equilibrium, making the protocol insecure. Game-theoretic security under the existence of multiple Nash equilibrium points is realized when following the protocol is Pareto-optimal/Focal equilibrium [2]. Stronger security guarantees are ensured if the equilibrium is Dominant Strategy Equilibrium (DSE) instead of Nash equilibrium (NE).

Network	**Threat Model**		
	$CFT(c)$	$BFT(t)$	$RFT(t,k)$
Synchronous	$2c < n$ [3]	$2t < n$ [4]	$t < \frac{n}{2}, k < \frac{n}{2}$ [4]
Partially-synchronous	$2c < n$ [3]	$3t < n$ [5]	$t < \frac{n}{4}, t+k < \frac{n}{2}$
Asynchronous	$c < \frac{n}{3}$ [6]	$t < \frac{n}{3}$ [6]	$t < \frac{n}{3}$ [6]

The results highlighted in blue are contributions of our work.

TABLE I
Bounds for consensus in different threat models.

There is an absence of protocols realizing ABC in the rational threat model. Our work addresses this gap and proves impossibilities and a novel protocol pRFT that achieves ABC in the rational threat model under certain conditions.

A. Our Contributions

We generalize the Rational Threat Model proposed in [1]. We classify the rational players into three types represented by different values of θ (representing player types). $\theta = 3$ is when rational players are incentivized to compromise liveness and cause censorship or disagreement. $\theta = 2$ is when rational players are incentivized only to cause censorship or disagreement, and $\theta = 1$ is when players are incentivized only to cause disagreement. Based on this for k rational, t byzantine players such that $t < t_0$ and total players are n, we present impossibility of consensus under non-standard byzantine assumptions for $\theta = 1, 2$. For $\theta = 3$, agreement is possible for $k + t < \frac{n}{2}$ and $t < \frac{n}{4}$ as achieved by proposed protocol pRFT.

- pRFT achieves consensus with $k + t < n/2$ and $t < n/4$ when rational players are of type $\theta = 1$.
- pRFT guarantees correctness (Dominant Strategy Equilibrium) and liveness in synchronous and partially synchronous network settings.
- We show that pRFT achieves optimal message complexity among consensus protocols that provide accountability.

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

Propose Phase:
if $i = r \bmod n$ **then**
  Block$_r$:= ConstructBlock$(\overline{tx}, r, b_{parent}, p_i)$
  $h_l :=$ Hash(Block$_r$)
  Broadcast$(\langle Propose, Block_r, h_l, r\rangle_i, s_i^{pro})$
else
  On Recv. $(\langle Propose, Block_r, h_l, r\rangle, s_l^{pro})$:
    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**
  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**
  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. $(\langle Reveal, h_j, s_l^{pro}, \overline{commit}_j, r\rangle, s_j^{rev})$:
  $M_i \leftarrow M_i \cup \{\overline{commit}_j\}$
  $D_i :=$ 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 $(\langle Expose, D_j, r\rangle, s_j)$
  Stash(D_j), $r := r + 1$
if $|D_i| > t_0$ **then**
  Broadcast$(\langle Expose, D_i, r\rangle_i, s_i^{expose})$
else if $|M_i| \geq n - t_0$ **then**
  Broadcast$(\langle Final, B_l, s_l^{pro}\rangle_i, s_i^{fin})$
else if $|F_i| > \frac{n}{2}$ **then**
  Broadcast$(\langle Final, B_l, s_l^{pro}\rangle_i, s_i^{fin})$
end if

Fig. 1. pRFT Protocol

Protocol	Message Complexity	Message Size	Accountability
pBFT [5]	$O(n^3)$	$O(\kappa \cdot n^4)$	×
Hotstuff [7]	$O(n^2)$	$O(\kappa \cdot n^3)$	×
Polygraph [8]†	$O(n^3)$	$O(\kappa \cdot n^4)$	✓
pRFT	$O(n^3)$	$O(\kappa \cdot n^4)$	✓

†While polygraph achieves same guarantees, their threat model is much weaker than pRFT's

Fig. 2. Message Complexity for consensus protocols compared with pRFT

II. Our Model

The system consists of $P = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n\}$ players which are divided into three disjoint types H — honest players, T — byzantine players and K — rational players. The system progresses in rounds, where in each round some value (in form of a block) is accepted. If nothing is accepted then empty block ($\perp$) is agreed upon.

Players. We omit discussing the utility of honest and byzantine players because they follow honest and arbitrary strategies, respectively, irrespective of payoffs. The k rational and t byzantine players that can form collusion of $\leq t + k$ size.

System States. The system states are: (1) σ_{NP} — no new blocks finalized, (2) σ_{CP} — censored transactions are not accepted in any round, (3) σ_{Fork} — two honest players agrees on different blocks and (4) σ_0 — honest execution.

Utility. Utility is based on current state σ, player type θ, player strategy π and *distinguisher function* $D(\cdot)$ that identifies deviation given the protocol and system state, and allocates corresponding penalty L. The utility is therefore given as $u_i(\pi, \theta, r) = \mathbb{E}_{\sigma \sim S}[f(\sigma, \theta)|\pi] - L \cdot D(\pi, \sigma)$.

III. Theoretical Results

We make the following theoretical contributions on RC in partially-synchronous setting. Explained in detail in [9]

- Rational consensus for $k+t < \frac{n}{2}$ and $t < \frac{n}{3}$ is impossible for rational players of type $\theta = 3$ or 2.
- There exists insecure equilibrium point for consensus protocol proposed in [1] which results in disagreement. This calls for more secure RC algorithms where game theoretic security should be through inexistence of any insecure equilibrium, rather than current notion of showing existence of secure equilibrium.
- Rational consensus for players of type $\theta = 1$ is possible. This existence proof is shown through construction of agreement protocol pRFT as shown in Figure 1. pRFT achieves consensus for $k + t < \frac{n}{2}$ and $t < \frac{n}{4}$.
- pRFT is an accountable protocol (detects and identifies deviating parties). It is at-par in communication complexity with currently best available solution [8] (see Table 2).

IV. Conclusion

This work proposes theoretical modeling of rational players to achieve ABC. We determine conditions under which RC is impossible and also propose protocol — pRFT which achieves RC for $k+t < \frac{n}{2}$ and $t < \frac{n}{4}$ under specific incentive structure of the rational players. The protocol is both accountable and has good communication complexity. However, the gap $\frac{n}{4} \leq t < \frac{n}{3}$ is still open and left for future work.

References

[1] A. Ranchal-Pedrosa and V. Gramoli, "Trap: The bait of rational players to solve byzantine consensus," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, (New York, NY, USA), p. 168–181, Association for Computing Machinery, 2022.

[2] T. C. Schelling, *The strategy of Conflict*. Oxford University Press, 1963.

[3] L. Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, p. 133–169, may 1998.

[4] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *J. ACM*, vol. 27, p. 228–234, apr 1980.

[5] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, (USA), p. 173–186, USENIX Association, 1999.

[6] G. Bracha, "Asynchronous byzantine agreement protocols," *Information and Computation*, vol. 75, no. 2, pp. 130–143, 1987.

[7] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus with linearity and responsiveness," in *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, PODC '19, (New York, NY, USA), p. 347–356, Association for Computing Machinery, 2019.

[8] P. Civit, S. Gilbert, and V. Gramoli, "Polygraph: Accountable byzantine agreement," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, pp. 403–413, 2021.

[9] V. Srivastava and S. Gujar, "Towards rational consensus in honest majority," 2024.