First, I'm NOT going to pick design decisions in the BAR paper and argue for a better design.

On the high-level, the BAR paper asks and answers the question of

how to design a BFT consensus protocol for multi-agent systems where the protocol **encodes an equilibrium** and **enforces the equilibrium** in the system.

Enforcing an equilibrium means that rational players prefer to obey, not deviate.

We wish to enforce an equilibrium because protocols should lead to stability, not chaos.

Before moving on, let me revisit the 3 concepts of equilibrium.

dominant-strategy (most restricted) ⊂ **Nash** ⊂ **correlated** (most general)

Using a social protocol to enforce a Nash equilibrium is the idea of correlated equilibrium.

The assumption in Nash is that every player knows how other players will play, meaning that when encoding a Nash in a social protocol and giving the protocol to a player, the protocol also encodes the information of how other players will play the game.

However, that is not always the case in real-world scenarios: consider the election game.

When designing an election rule as a social protocol, it doesn't encode the information of how different players will play the game (i.e., how different voters will vote).

Therefore, this kind of protocols can only enforce a restricted concept of equilibrium.

And this restricted concept is dominant-strategy equilibrium, meaning, for each player, there exists a single best action to take, regardless of other players' actions.

The question that my research is trying to ask is

Whenever we formulate a real-world scenario into a game form

meaning, we specify who are the players, what actions they can take, how to map players' actions to the game's outcome and how players feel about different outcomes

we will realize that many games have **multiple** equilibriums.

So how to choose which equilibrium to encode? Are there general guiding principles?

This question is different from but related to the question that BAR asks.

Before answering, here's an intuition of why my research is asking this question.

Recall our OSDI paper, the lesson of election games tells us that the only way to enforce a dominant-strategy equilibrium is dictatorship. All other election rules are manipulable.

But people may not want to enforce dictatorship as the social protocol.

This inspiration we got has the flavor of which equilibrium NOT to choose for a protocol.

One general guiding principle is (I suggest this in a humbled way)

to protect the weak and to constrain the strong.

On the one hand, "without oligarchy" is in a sense moving towards this principle.

On the other hand, recall the real-world issue: stronger wall-street banks use secret and faster networks between NYC and Chicago to front-run weaker financial companies.

Our application domain is calling for this principle to be implemented!

A principled approach of choosing which equilibrium to enforce in a system:

It is impossible to enforce a dominant-strategy equilibrium by any consensus protocol.

If we still wish to enforce an equilibrium, we can enforce the more general concept, Nash.

Since encoding a Nash into a protocol requires encoding the information of how other players will play the game, we need the latency (distribution) matrix to start our design.

To protect the weaker players, we use this matrix to infer the client-side invoke ordering.