On the high-level,

the BAR paper asks and answers the question of how to design a BFT protocol for distributed, multi-agent systems where the protocol

encodes an equilibrium and enforces the equilibrium in the system.

Enforcing an equilibrium means that rational players in the system will prefer to obey.

We want to enforce an equilibrium -- protocol leads to stability instead of chaos.

I think the BAR paper gives a nice and comprehensive answer.

My research tries to ask a related but different question.

Before I move there, let me revisit the concepts of equilibrium.

In game theory, dominant-strategy \subset Nash \subset correlated.

The assumption in Nash is that every player knows how other players will play, meaning that if we encode a Nash into a protocol, the protocol also encode the information of …

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

When designing an election rule as a social protocol, it doesn't encode the information.

This kind of protocol can only enforce a restricted concept of equilibrium.

This restricted concept is dominant-strategy equilibrium. But there is an impossibility.

The question my research tries to ask is

When we formulate a real-world situation into a game form

(players, actions, outcome), and try to use equilibrium for analysis,

we will realize that there exists *multiple* equilibriums.

It is unclear how to choose which equilibrium to encode (traffic light).

Further, I wish to ask: Are there general guiding principles of how to choose …?

This is a related but different question from BAR.

Before showing my answer, an intuition of why my research is asking this question

Recall our OSDI paper, the lesson of social choice theory tells us that the only …

People may not want to enforce dictatorship as the social protocol, but (since only)…

This inspiration has the flavor of which equilibrium NOT to choose in a protocol.

One general guiding principle (I say it in humbled way)

is to protect the weak and to constrain the strong.

On the one hand, when we talk about without oligarchy, it has the flavor …

On the other hand, last week, we talked about what happened in the real-world:

Stronger wall-street banks use secret and faster network between NYC and Chicago to front-run and screw up weaker financial companies.

The application calls for the system to protect the weak and constrain the strong.

I don't know what you feel; I feel that this doesn't sound bad as a principle.

A principled approach of choosing an equilibrium

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

If we still wish to enforce an equilibrium, we need to use the more general 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.

Enforcing the matrix and Recover the client-side order is trying to pursue the principle.