Discussion of: *An Economic Model of Consensus on Distributed Ledgers*

by

Hanna Halaburda, Zhiguo He, and Jiasun Li

Discussant: Yackolley Amoussou-Guenou

Inaugural Annual Conference DeFi & Digital Currencies
WBS Gillmore Centre for Financial Technology
2 September 2022, London

System Studied

- System considered is inspired by protocols used by majority of PoS blockchains
  - Committee of nodes, a leader sends a message to all other nodes
  - Nodes broadcast back the leader's message to the others (a vote)
  - Commit or not, depending on #messages received locally

- Problem solved: All nodes atomically "commit" the good reception

- Frequent assumption in CS: nodes are either honest or Byzantine

System Studied

- System considered is inspired by protocols used by majority of PoS blockchains
  - Committee of nodes, a leader sends a message to all other nodes
  - Nodes broadcast back the leader's message to the others (a vote)
  - Commit or not, depending on #messages received locally
- Problem solved: All nodes atomically "commit" the good reception
- Frequent assumption in CS: nodes are either honest or Byzantine
- Actually: All **non-Byzantine** nodes atomically "commit" the good reception
  - These protocols are said to be BFT protocols which stands for Byzantine-Fault Tolerant

But in DLTs' Application…

- Nodes usually have some economic/financial desires and interests
- Need to study if these protocols work with rational utility maximiser nodes
  - Alternatively, what are the incentives of rational nodes in these protocols
- **This paper proposes an incentive analysis of BFT protocol**

Settings of the Paper

- n nodes. 1 is chosen at random and is the leader
- f nodes in the committee are Byzantine nodes (arbitrary behaviours)
- The rest, $n - f$ are rational and ambiguity averse about who are the Byzantine and their actions
  - They max – min on all possible outcomes

Actions and Objectives

- A rational proposer
  - Send message to the other nodes with iid probability $p \in [0,1]$. **Choose p**
- The other nodes, called backup
  - If message received, echo to the others with iid probability $q \in [0,1]$. **Choose q**
- Byzantine nodes choose to whom to send its message/votes (possibly to none)
- After the "echo" phase
  - Commit or not according to the #messages received (leader's + echoes)

Actions and Objectives

- A rational proposer
  - Send message to the other nodes with iid probability $p \in [0,1]$. **Choose p**
- The other nodes, called backup
  - If message received, echo to the others with iid probability $q \in [0,1]$. **Choose q**

	"Almost all" commits	**Otherwise**
The node commits	$R > 0$	$-c < 0$
The node does not commit	0	0

Actions and Objectives

- A rational proposer
  - Send message to the other nodes with iid probability $p \in [0,1]$. **Choose $\boldsymbol{p}$**
- The other nodes, called backup
  - If message received, echo to the others with iid probability q $\in [0,1]$. **Choose $\boldsymbol{q}$**

	"Almost all" commits	Otherwise
The node commits	$R > 0$	$-c < 0$
The node does not commit	0	0

- **This paper analyses and presents all the <u>symmetric</u> PBE of this game**
  - With no message loss and when messages can be lost
  - Continuum of nodes, i.e., a single node (measure 0) strategy does not affect the outcome

Summary of the Main Results

- There always exist babbling equilibria in which no rational node commits

Summary of the Main Results

- There always exist babbling equilibria in which no rational node commits

- Other symmetric equilibria if R is high enough
  - If $p = 1$, in the equilibria, conditions of commit decisions depends on whether the leader's message is received or not

Summary of the Main Results

- There always exist babbling equilibria in which no rational node commits

- Other symmetric equilibria if R is high enough
  - If $p = 1$, in the equilibria, conditions of commit decisions depends on whether the leader's message is received or not
    - Does not hold in idiosyncratic loss of message
    - Holds in systematic loss. Depending on the value of π odes can infer the system's state

Idiosyncratic loss: all messages have the same probability α of being lost

Systematic loss: natures chooses (1) if all messages will be delivered as if no loss of messages, with probability π or if (2) each message sent has a probability α of being lost, with probability $(1 - \pi)$

Summary of the Main Results

- There always exist babbling equilibria in which no rational node commits

- Other symmetric equilibria if R is high enough
  - If $p = 1$, in the equilibria, conditions of commit decisions depends on whether the leader's message is received or not
    - Does not hold in idiosyncratic loss of message
    - Holds in systematic loss. Depending on the value of π odes can infer the system's state
  - If $p < 1$ and is in a specific interval, in the equilibria, commit decisions depends only on messages received

Idiosyncratic loss: all messages have the same probability α of being lost

Systematic loss: natures chooses (1) if all messages will be delivered as if no loss of messages, with probability π or if (2) each message sent has a probability α of being lost, with probability $(1 - \pi)$

Summary of the Main Results

- There always exist babbling equilibria in which no rational node commits

- Other symmetric equilibria if R is high enough
  - If $p = 1$, in the equilibria, conditions of commit decisions depends on whether the leader's message is received or not
    - Does not hold in idiosyncratic loss of message
    - Holds in systematic loss. Depending on the value of π odes can infer the system's state
  - If $p < 1$ and is in a specific interval, in the equilibria, commit decisions depends only on messages received

- These equilibria hold for any $q > 0$

Idiosyncratic loss: all messages have the same probability α of being lost

Systematic loss: natures chooses (1) if all messages will be delivered as if no loss of messages, with probability π or if (2) each message sent has a probability α of being lost, with probability $(1 - \pi)$

I really like the paper

- The contributions of the paper are well presented, and mostly nicely motivated
- The paper presents the advantage of echoing the leader's message (peer-to-peer communication) and its importance for building these systems
- The contributions and implications are well presented and make parallels with either CS literature, or (potential) practitioner uses
- …

CS Literature – Distributed Computing

- Definition of the paper
  - Consensus on message succeeds … if and only if “almost all” rational nodes commit. Otherwise, consensus fails
- Different to the CS definition of consensus: Termination, Agreement and *Validity*
- Close to another central problem in CS: the (Byzantine) Reliable Broadcast
  - If an honest "leader" sends a message, all honest should commit
  - If a Byzantine "leader" sends a message, either
    - All honest nodes commit, or
    - No honest node commits
- Moreover, in this paper the problem seems to be of a probabilistic nature

https://connorzanin.com/bft-broadcast/

Case of message loss

- Aren't the two following cases similar
  1. No message loss but $p < 1$. I.e., p cannot be equal to 1, and
  2. Idiosyncratic message losses

- Systematic risk of message loss does not seem well motivated in the paper. Seems less realistic than idiosyncratic case, but
  - Can correspond to disasters (natural, a network cable damaged, …)
  - Affect the network, but those events are not known in advance

- What would happen on these results if the probability of losing messages where not symmetric (e.g., two nodes have a better connection and a bad with others)

Notion of Continuum of Nodes

- Key to the analysis
- Could benefit from more discussion and motivation
  - Strategy of a single rational node does not affect the consensus
  - However, the set of nodes is discrete
- In most BFT blockchains, committees' size in small
  - System's latency increases with the number of nodes
  - Reliable broadcast is more scalable → a single node has less impact

Some Other Comments

- If messages are lost, what happens if the nodes are also averse to reception

- In CS, designer chooses the parameters to solve the problem in all scenarios
  → For this problem, $p = 1$
  - But due to real life limitations, some node cannot receive message in time
  - Is that the motivation of having p and q in this model?

- Case of costly operations?
  - While message seems light, in DLTs, blocks are heavy and costly to send
  - Commit is a signal of good reception
  - Checking validity of the information to add usually requires costly computations

Merci | Thank you