Discussion of **Auer, Monnet and Shin's** ***Permissioned Distributed Ledgers and the Governance of Money***

Hanna Halaburda (NYU)

CB&DC Virtual Seminar, 26 March 2021

INCENTIVES IN PERMISSIONED BLOCKCHAIN

- timely topic
  - after permissionless, we finally look closer at permissioned systems
- first to analyze the incentives in permissioned system in such a detail
- we learn a lot about the forces
  - also illustrates the general issues that we are up against in analysis of permissioned blockchains

- three parts in this paper
  - model of trade (credit to late producers)
  - **validation game**
  - optimal design: number of validators, τ , compensation, etc

VALIDATION GAME – TWO STAGES

1. label validation
   - verify the label of producers
   - vote by sending a message
2. production validation
   - verify whether production took place according to plan
   - vote by sending a message

- verification and sending messages is costly
  - validators need to be compensated
  - they are also subject to bribes
- payoff only if τ of validators validates a good state

$\Longrightarrow$ coordination game

  - solved by a global game with variable cost as private information
- higher τ limits incentives for bribes, so makes the system more secure, but also makes preventing free-riding more costly

WHAT IS “THE LEDGER” IN A DISTRIBUTED SYSTEM?

- all validators (nodes) keep a copy — but the copies can differ
- if all nodes are equal (and opportunistic), maintaining consistency of the ledger between the nodes is the major challenge
  - voting? who would tally the votes? do you trust them?
  - *local voting*: all nodes send their votes to all other nodes, so everyone tallies the votes
    - but nodes can send different votes to different recipients
    - my tally may be different than your tally
    - need multiple rounds to reconcile and make sure we all update the ledger the same way
    - this is why BFT so much more complicated than just voting
- if one node is more important than others (*notary*), this node keeps the authoritative copy (“the ledger”), and tallies validators’ votes
  - do we trust this node to write in “the ledger” what the nodes have voted for?
  - what do validators do that the notary cannot?

WHAT DO WE NEED THE VALIDATORS FOR?

- what benefits do we expect from a decentralized system in a permissioned setting?
    - a consensus where no node is more important than another?
        - not in this setting, because we have the *notary* node
    - validators checking consistency of the ledger by keeping the *notary* node in check from misreporting?
        - what would happen if after validators vote, the *notary* writes a different value to the ledger?
    - validators aggregating some dispersed information from outside of the ledger (i.e., oracles)?
- whatever we expect, we should NOT expect cost savings
    - redundancy of operations (and cost) is necessary in distributed systems

WHAT DO VALIDATORS BRING TO THE VALIDATION GAME?

1. label validation
   - verify the label of producers – *which they read from the ledger*
   - vote by sending a message *to the ledger*
   - *wasn't this information already there?*
2. production validation
   - verify whether production took place according to plan
     - ★ do they actually observe the production, sensor readings?
     - ★ do they all observe the same data or a noisy signal?
     - ★ is it something that the notary cannot observe directly?
     - ★ what is the benefit of the redundancy?
   - vote by sending a message

- economic benefits? why is decentralization and redundancy beneficial? we know it is more costly
- cannot be modeled separately

IDENTITY AND INCENTIVES IN PERMISSIONED SYSTEMS

- are validators' identities known?
- the producer knows their identities if he can target the bribes
- validators would benefit from colluding even without bribe
  - if they collude and incorrectly claim that B producer is a G producer, they get z^1 instead of 0

- punishment – with probability π misbehaving validators are caught
  - who catches them?
  - why not punish them more than just exclusion? if you put high enough fine on them, you can prevent misbehavior more effectively

SUMMING UP

- great, detailed paper
- extremely important
- gets us thinking about the incentives and optimal design
- as well as challenges in analyzing permissioned blockchains
    - modeling the benefits of decentralization in a permissioned setting