# DLT and Financial Markets

CEPR and INSEAD Fintech Webinar, September 15, 2020

Hanna Halaburda

# Appeal of Blockchain

- excitement is driven by the belief that
  - an **immutable** and **decentralized** system is desirable,
  - as it would **prevent fraud** and lead to **democratization of services**

# However…

permissionless cryptocurrencies…

- are **not** immutable
  - the safety of the PoW blockchain is directly link to the cost of mining
    - cost of mining is the cost attack
  - if the value that can be double-spent is larger than the cost, it is worthwhile to attack
  - the most ``wasteful'' cryptocurrencies are the most secure
- can achieve only **limited** decentralization in equilibrium
  - mining is risky and costly, and different miners have different mining cost
  - mining pools — risk aversion
  - without mining pools — ``cheaper'' miners will get a larger share of mining

(known in the literature, cf research by Cong, Li & He; Arnosti & Weinberg; Moroz, Narula & Parkes; and E.Budish; we also document it in *The Microeconomics of Cryptocurrencies*, Halaburda, Haeringer, Gans & Gandal)

# Permissioned blockchain may deliver more decentralization

(Halaburda & Mueller-Bloch, 2019; Bakos, Halaburda & Mueller-Bloch, forthcoming)

- common misperception:
  - permissionless blockchains are more decentralized than permissioned
- permissionless systems, in principle, may **allow** for arbitrary level of decentralization
  - but they cannot guarantee any level of decentralization
  - in equilibrium the level of centralization depends on the cost of participating (e.g., development is more costly than mining, and is more centralized)
- permissioned systems can **guarantee** a certain level of decentralization
  - it can be higher level than the equilibrium in permissionless

# Smart contracts, immutability and permissioned blockchain

(Halaburda & He, in progress)

- financial transactions often involve mistakes
  - fat-finger transactions (cryptocurrencies)
  - mistaken oracles (smart contracts)
- immutability may not be so desirable for a large-scale financial system
- instead system that is **secure** and **flexible**
  - validator(s) would reverse mistaken records
  - and would be restricted from self-serving abusive changes

# How to achieve secure and flexible system?

(Halaburda & He, in progress)

- permissioned blockchain, with a limited number of known and accountable validators

- the more validators there are, the more costly it is to change records
  - both permissionless and permissioned
  - both mistake records and ``good" records
- validators in permissioned system subject to external accountability
- permissionless (-> pseudonymous) — no external accountability
- validators would change "good" records for private gain (e.g., double-spending or misappropriation)
  - no private gain from changing a mistake records

# How to achieve secure and flexible system? (cont'd)

(Halaburda & He, in progress)

Results:

- permissionless
  - never want to change mistake records (no flexibility)
  - if lots of validators, larger payments are safer (security)
- permissioned, due to accountability
  - for the same number of validators, even larger payments are safer (more security)
  - if not too many validators, will change mistake records (flexibility)

# Decentralization of financial services?

(Halaburda & Gottesdiener, in progress)

- would smart contracts (with DLT) allow for decentralization of financial services?
  - not really
- smart contracts would need to favor small players more than the large players
- smart contracts offer cost savings due to automation
  - larger players can take advantage more
- smart contracts do not offer “decentralization of trust” (decentralization of risk)
  - insurance example
  - generalizes to any financial services with risk, where diversification helps

Thank you!