# Permissioned Distributed Ledgers and the Governance of Money

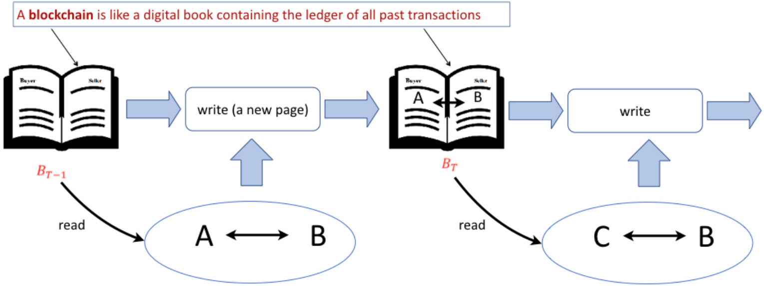
Raphael Auer    Cyril Monnet    Hyun Song Shin

25 March 2021

# "Money is memory"

- Money is a record of goods sold and of services rendered
  - Alternative to a **ledger** that records the complete history of all transactions
  - Kocherlakota (JET 1998) "*Money is memory*"
- Lugging around a universal ledger was a fanciful notion; a theoretical construct, more than a practical one
- But have advances in computing and cryptography brought such a ledger closer to reality?

# Blockchain as a ledger



# Distributed ledgers or centralised ledgers?

- Robustness that derives from **redundancy**
  - Not only about keeping copies of the ledger in a safe place
- Governance
  - **Checks and balances** on operators of the system
  - Avoids "all-in" risk; there is more than one basket for the eggs

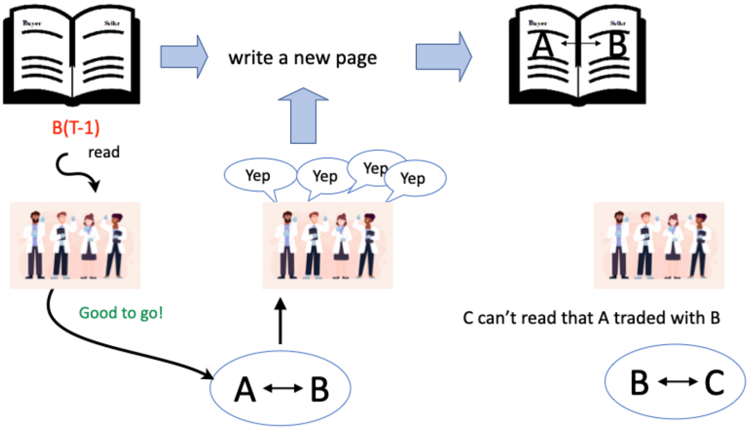
But advantages of distributed ledgers do not come cheap

- **Incentive costs** to maintain the monetary equilibrium as a robust equilibrium (eg, Proof of work in bitcoin protocol)

# Permissionless and permissioned distributed ledger technology (DLT)

- Permissionless DLT
  - eg, Bitcoin (Nakamoto (2008)); suported as an equilibrium (Biais et al. (RFS 2019))
  - But well-known limitations as money (BIS (2018), Chiu and Koeppl (2017), Budish (2018))
- Permissioned DLT
  - Supermajority (typically, 75-80 percent) is arbiter of truth; what is true or not is a matter of what the supermajority of the validators say it is
  - Potential applications for central bank digital currency (CBDC), trade finance, securities settlement
  - Equilibrium properties are becoming better known (eg, Amoussou-Guenou et al. (2019) when there are "Byzantine" players)

# Permissioned distributed ledger



# Our paper

- Economy with scope for gains from production and exchange
- **How many validators** operate the distributed ledger?
- Reconciled ledger that records the past truthfully is a public good
  - How to incentivise validators?
  - How to ensure validation of honest histories only?
- **Public good contribution game** formalised as a **global game**

# Two forces at work

1. Strong governance requires many validators and high supermajority threshold for consensus
   - It is more expensive to pervert history with many validtors than that of one
2. But, having high supermajority threshold entails **higher rents** to overcome free-riding incentives
   - Unanimity is an impossibly high standard
   - Economic gains are dissipated in sustaining decentralised consensus

# What we do

- Solve for optimal number of validators and supermajority threshold
- Finding: centralised ledger is generally superior, unless weak governance necessitates decentralised consensus

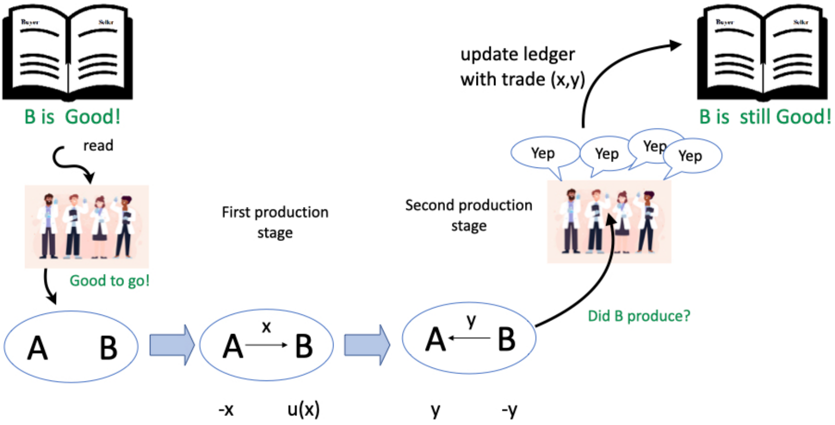
# Model

- $t \in \{0, 1, 2 \cdots\}$; discount factor is $\beta \in (0, 1)$
- Each period divided into two production stages
- Agents are of two (permanent) types: early and late producers, randomly matched
- Allocation $(x, y)$; first best is $x^*$ where $u'(x^*) = 1$
  - Without commitment, one-shot equilibrium is autarky $x = y = 0$
- **Need a ledger!**
- Chiu and Koeppl (RFS, 2019)

# Ledgers: recording past behaviour

- The ledger records in each period $t$:
  - Agreed allocation $(\widetilde{x}_t, \widetilde{y}_t)$
  - Realised $(x_t, y_t)$
- Late producers can be either in good $(G)$ or bad $(B)$ standing
  - Standing $B$ if, in the past, they failed to keep to agreement; if $\widetilde{y}_s \neq y_s$ for some $s \leq t$
  - Standing $G$ otherwise
- Some late producers are "faulty" and cannot produce
  - proportion $f$ of faulty producers (with $B$ label)
- Validators are chosen from late producers
  - Early producer cannot tell $G$ from $B$

# Verification, production, and validation



# Validators' collective action problem

- Each validator chooses to **work** or **shirk**
  - **Work** entails verifying and communicating labels; incurs cost $\chi_i > 0$
  - Provided that supermajority $\hat{\kappa}$ **work**, the reports coincide and each collects share of surplus $(1 - f)\,z > 0$
  - **Shirk** entails no cost and no benefit (cannot accurately fake honest reports)
- Payoff to **work**

$$\begin{cases} (1-f)\,z - \chi_i & \text{if } \kappa \geq \hat{\kappa} \\ -\chi_i & \text{otherwise} \end{cases}$$

- Payoff to **shirk** is zero

# Public good contribution game

- Payoff to work is

$$\begin{cases} 1 - c_i & \text{if } \kappa \geq \hat{\kappa} \\ -c_i & \text{if } \kappa < \hat{\kappa} \end{cases}$$

  where

$$c_i = \frac{\chi_i}{(1 - f)\, z}$$

  Payoff to shirk is zero

- Cost $c_i$ similar across validators

$$c_i = \theta + \eta_i$$

  where $\theta$ has support $[0, 1]$ and $\eta_i$ is uniform i.i.d. over $[-\varepsilon, \varepsilon]$ for small $\varepsilon > 0$

# Solution

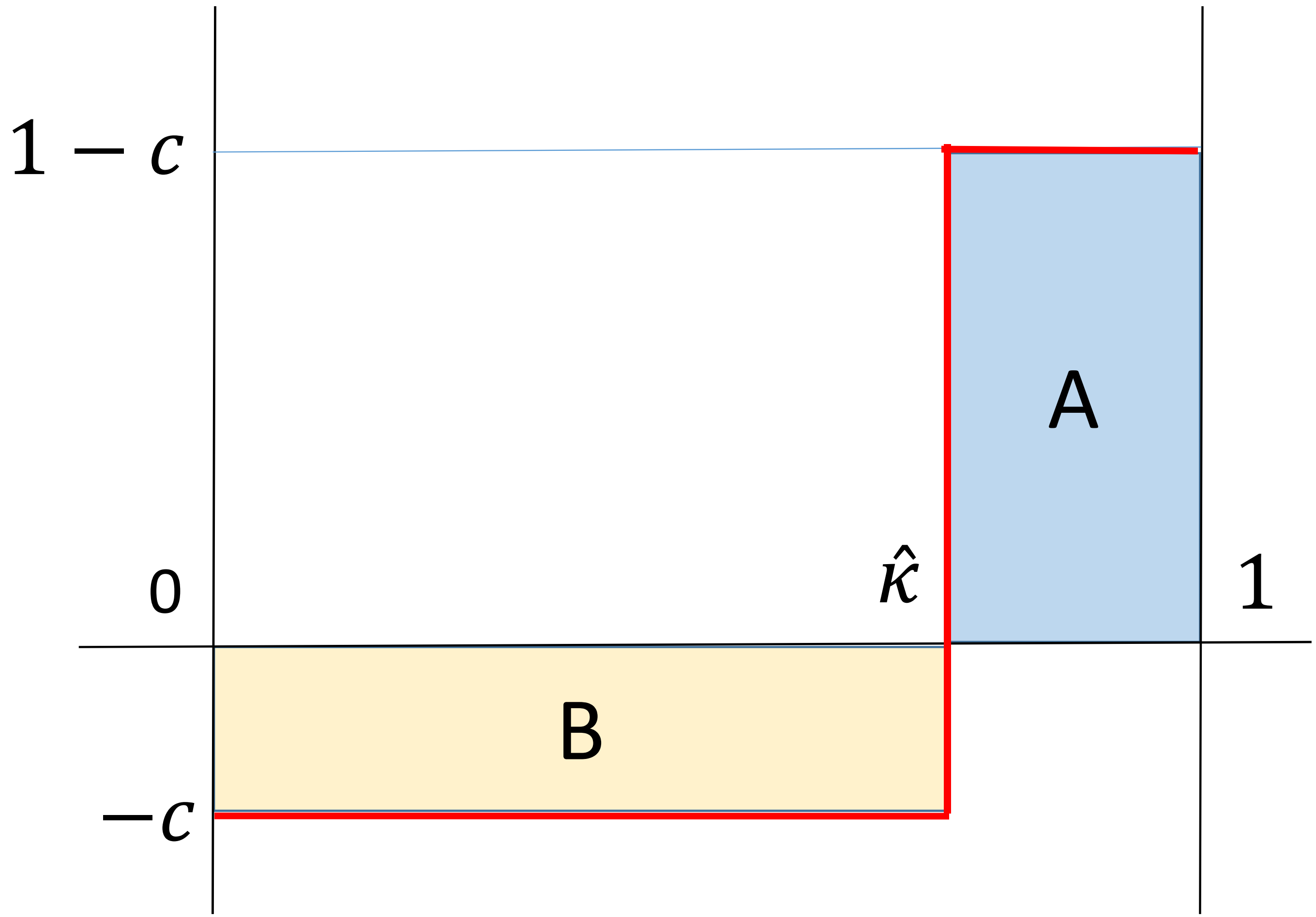
**Lemma**

*Suppose all validators follow switching strategy:*

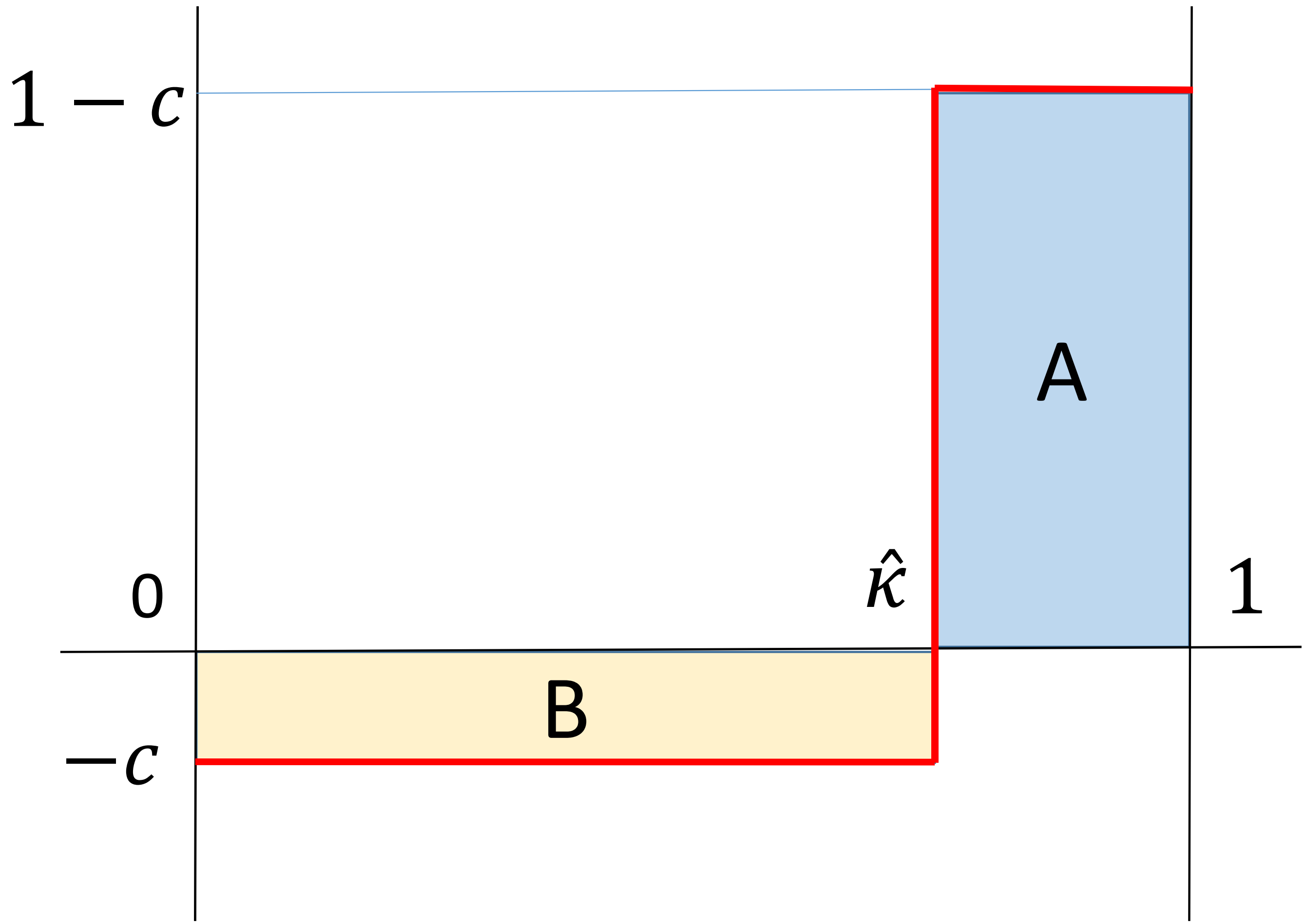
$$s(c_i) = \begin{cases} \textit{work} & \textit{if } c_i \leq c^* \\ \\ \textit{shirk} & \textit{if } c_i > c^* \end{cases}$$

*where $c^*$ is interior. Then, in the limit as $\varepsilon \longrightarrow 0$, the density of $\kappa$ conditional on $c_i = c^*$ is uniform over $[0, 1]$*

So, in the limit as $\varepsilon \longrightarrow 0$, all validators have the same cost, but the conditional density of $\kappa$ at the switching point is uniform (Morris and Shin (1998, 2003))



1 − c
A
0
κ̂
1
B
−c


1 − c
A
0
κ̂
1
B
−c

# Solution

- Payoff to work given cost $c_i = c^*$ is

$$\begin{aligned} & -c^* \Pr\left(\kappa < \hat{\kappa} \middle| c^*\right) + \left(1 - c^*\right)\left(1 - \Pr\left(\kappa < \hat{\kappa} \middle| c^*\right)\right) \\ = \;& \left(1 - c^*\right) - \Pr\left(\kappa < \hat{\kappa} \middle| c^*\right) \end{aligned}$$

  while payoff to shirk is zero
- From lemma on uniform density of $\kappa$ at the switching point, we have $\Pr\left(\kappa < \hat{\kappa} \middle| c^*\right) = \hat{\kappa}$
- So, solution is

$$c^* = 1 - \hat{\kappa}$$

# Solution

## Theorem

*In the limit as* $\varepsilon \to 0$*, there is a unique, dominance-solvable equilibrium where the public good is provided if and only if*

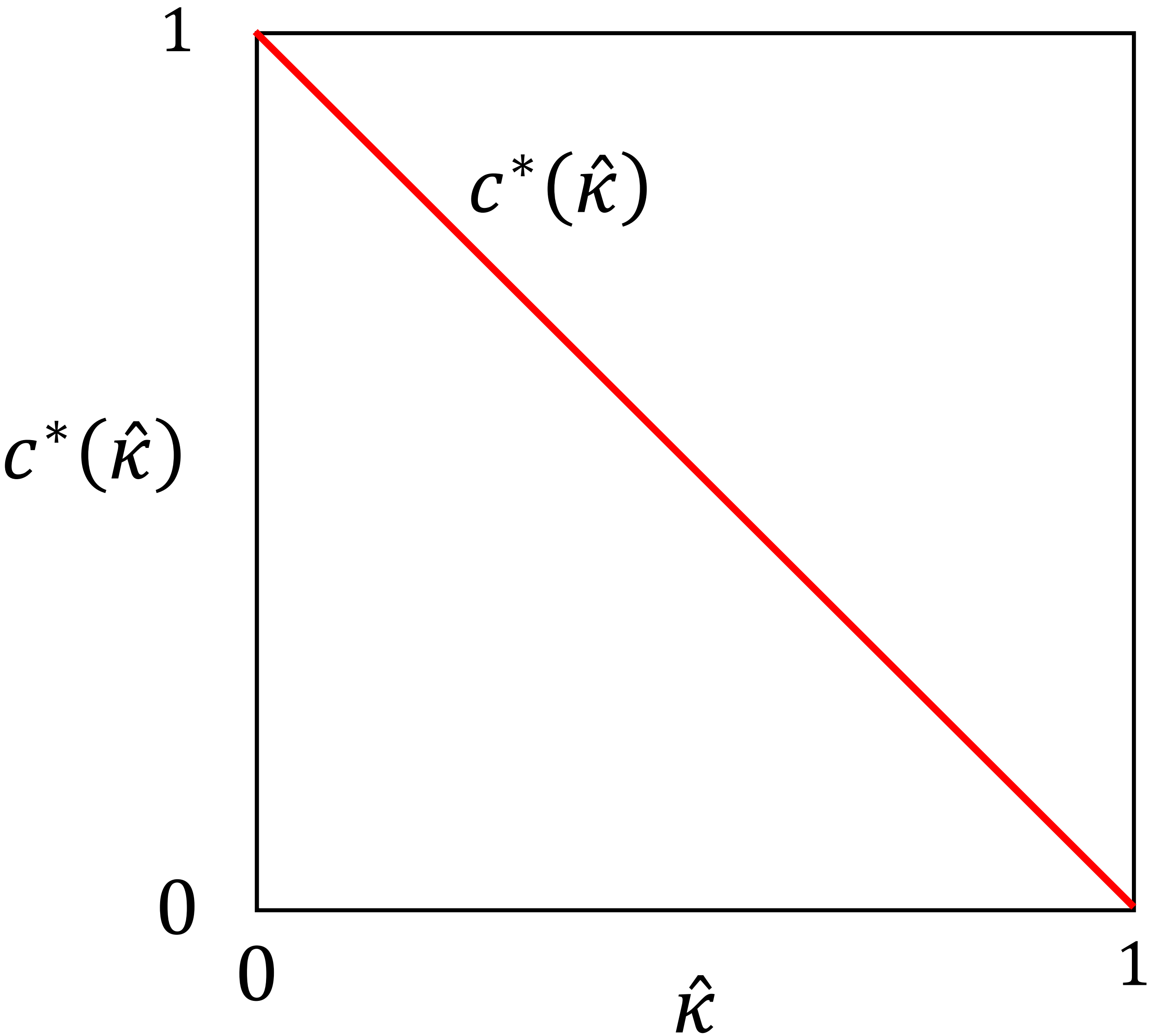
$$c \leq 1 - \hat{\kappa}$$

## Corollary

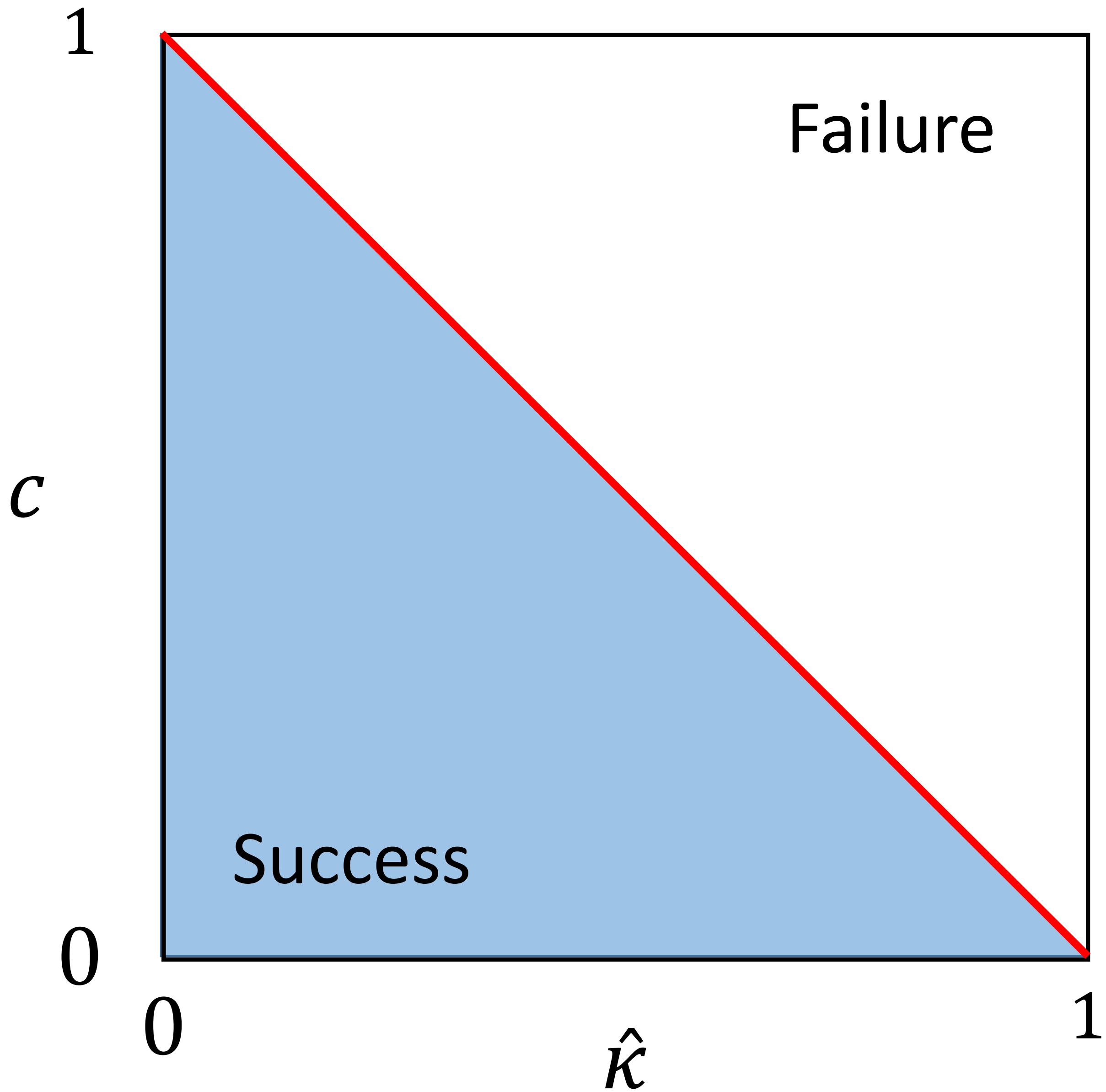
*Public good is never provided when unanimity is required*

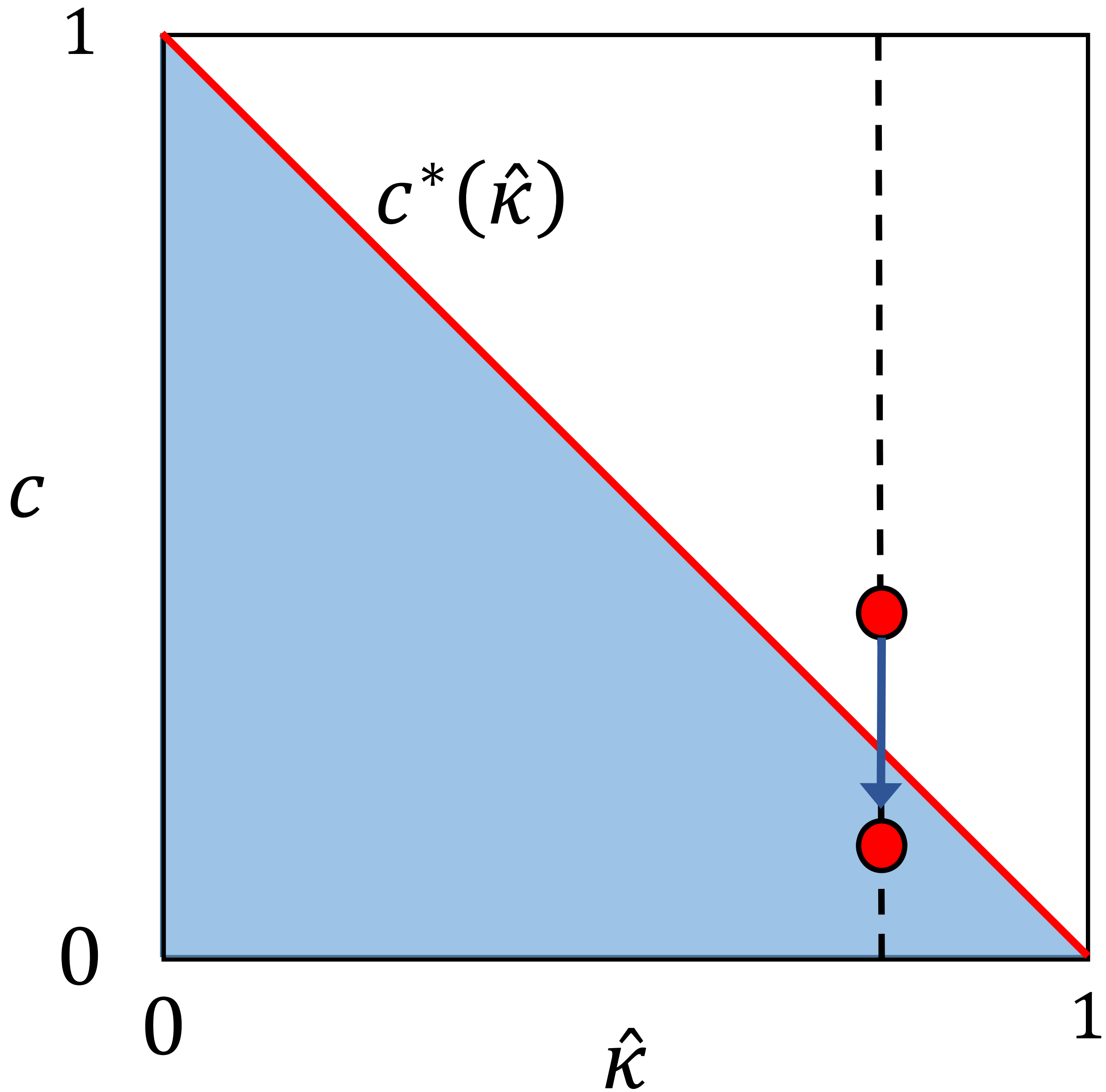
## Corollary

*Public good provision implies higher rents (high* $z$*) for validators as* $\hat{\kappa}$ *rises*



1
$c^*(\hat{\kappa})$
$c^*(\hat{\kappa})$
0
0
1
$\hat{\kappa}$

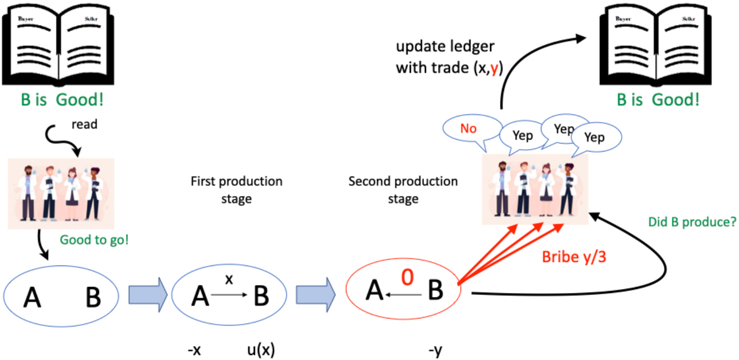

1
Failure
$c$
Success
0
0
$\hat{\kappa}$
1



1
$c^*(\hat{\kappa})$
$c$
0
0
$\hat{\kappa}$
1

# Optimal number of validators with side-payments

- Many validators and high supermajority threshold guards against manipulation using side payments
- But high supermajority threshold not sustainable with fundamental uncertainty



# Solution

- $\pi$ is probability that bribe is uncovered; $\alpha$ is probability of match; $\beta$ is discount factor

$$\delta \equiv \frac{\pi\beta\alpha}{1-\beta}$$

Proposition 2. Optimal monetary arrangment depends on $\delta$, with thresholds such that:

- High $\delta \Rightarrow$ single validator is optimal
- Moderate $\delta \Rightarrow$ permissioned distributed ledger is optimal
- Lower $\delta \Rightarrow$ permissionless distributed ledger is best
- Very low $\delta \Rightarrow$ no economic gains can be reaped

# Lessons

- **Main result:** maintaining monetary equilibrium entails rents for validators that are high enough to sustain monetary equilibrium as a robust equilibrium

Two consequences:

- **A general inefficiency result**: the economic gains from the institution of money cannot be reaped if the economic gains are not sufficient to cover the incentive costs
- **Distributional consequences:** if the economic gains are large enough to sustain monetary equilibrium, the gains accrue to validators first and users come second