Blockchain Design with Transmission Delays

Michele Fabi

Ecole Polytechnique CREST IP Paris

September 21, 2023

X-OMI Workshop on Blockchain and Decentralized Finance

What is a Blockchain?

- A blockchain is a distributed and decentralized computer.

- A blockchain is distributed:

  A network of (blockchain) miners runs multiple servers simultaneously.

  Each server records its own history of operations .

- A blockchain decentralized:

  No central authority.

  Miners act based on their incentives within hard-coded protocol rules.

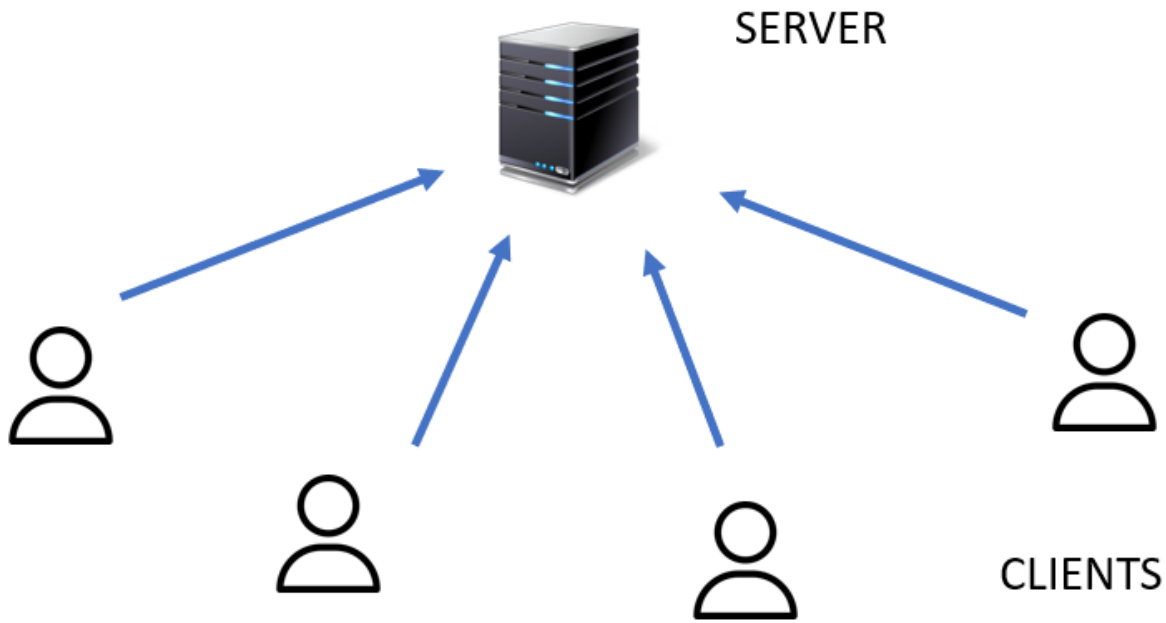
What is a Blockchain?

- A blockchain is a distributed and decentralized computer.

- Modern blockchains support Turing-complete programming languages.

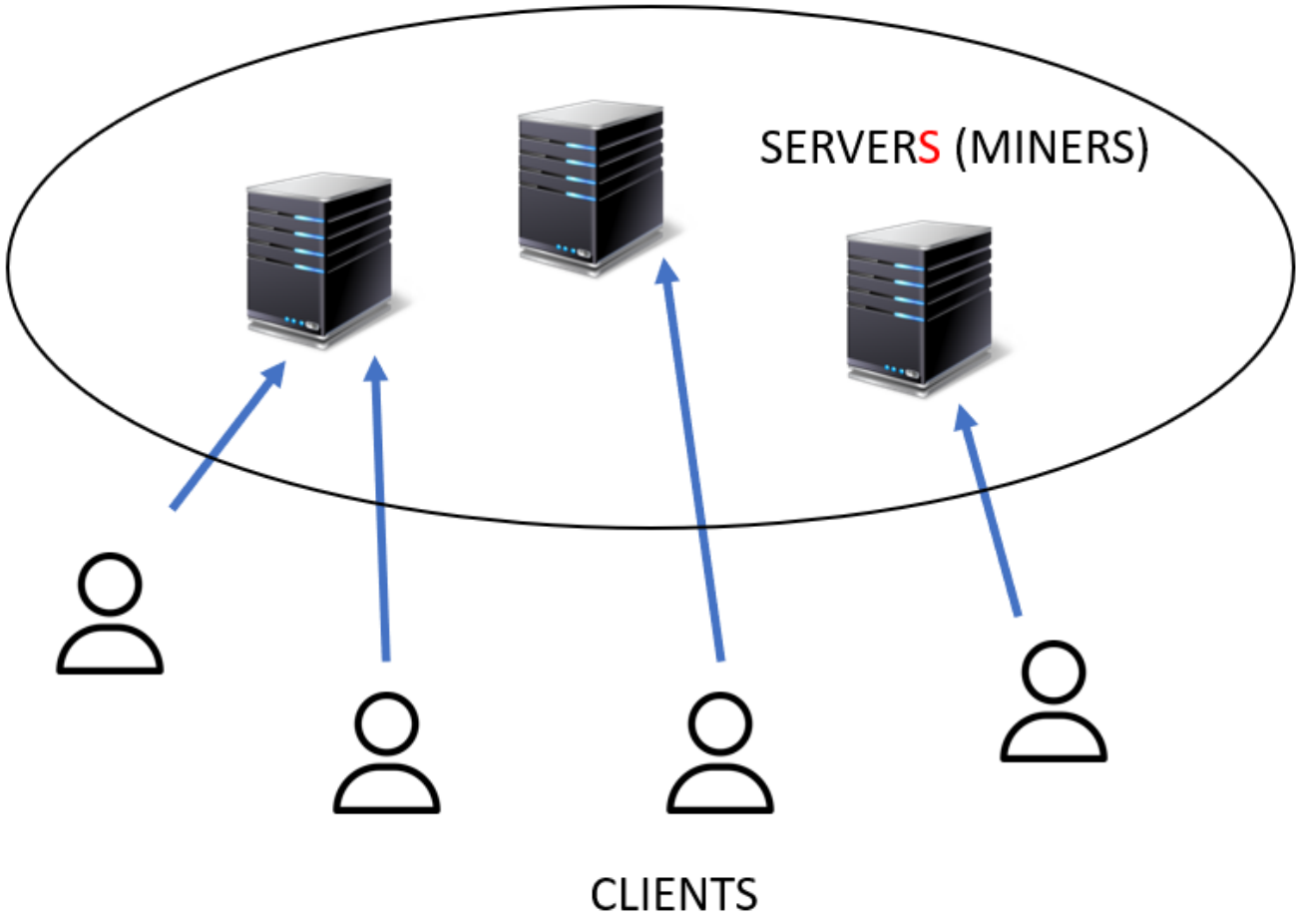
  With smart contracts, they can perform operations beyond recording payments (old idea of blockchains as ledgers).

Single-Server Infrastructure (Centralized)



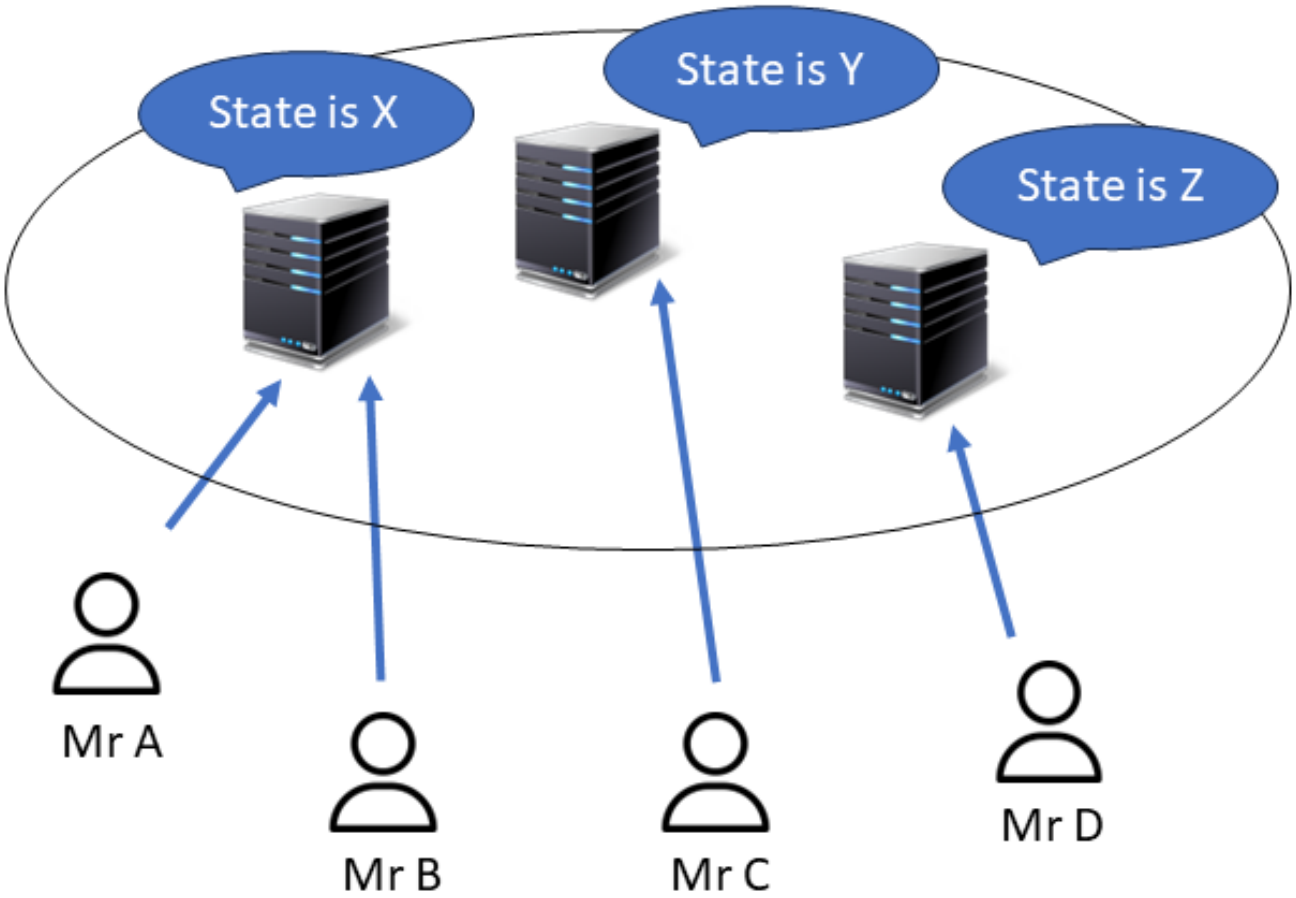
- Single, authoritative record of all transactions.

Multi-Server Infrastructure (Blockchain)



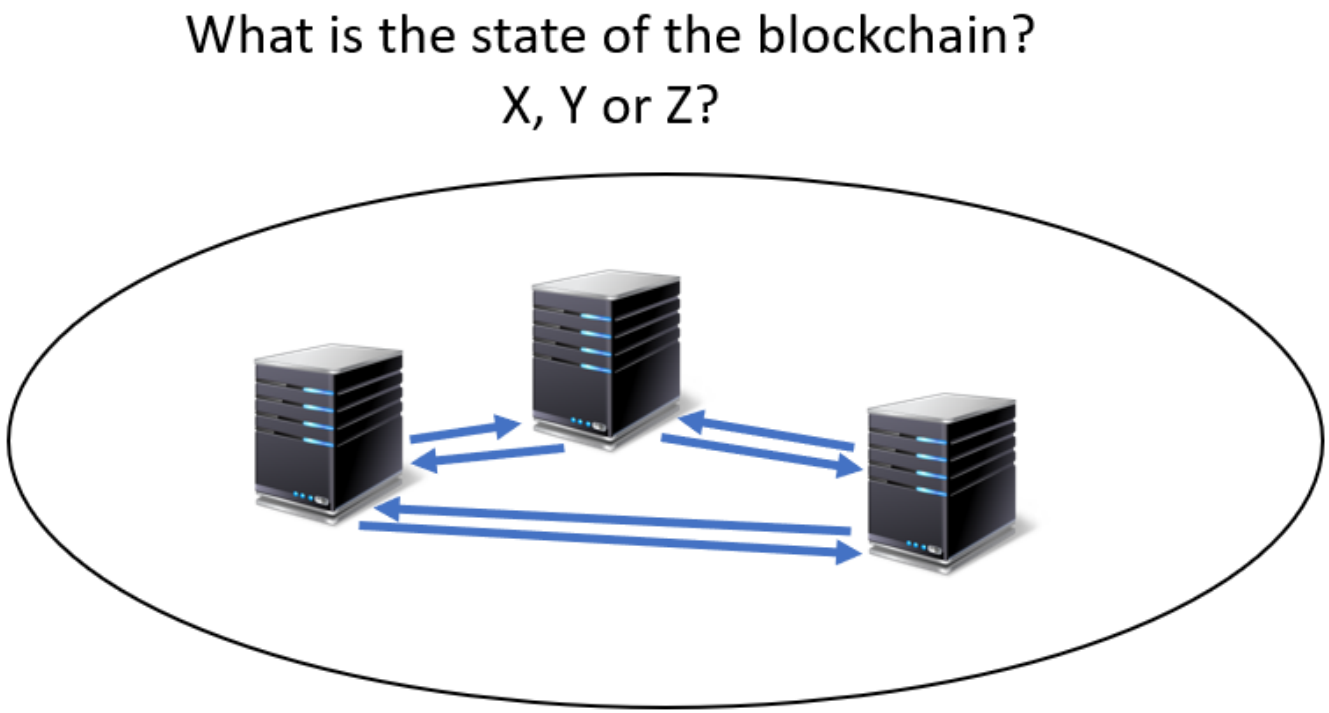
- Multiple servers (stored by miners) co-exist at the same time.

Consensus Problem



- Miners can record conflicting states.

Consensus Problem



- Miners have to communicate and agree on a unique state of the blockchain.

- This is the problem of distributed consensus.

  It is addressed by miners' consensus protocol.

Nakamoto Consensus

- The most popular consensus protocol (for blockchains) is Nakamoto consensus

- Miners record transactions batched into blocks.

  Then they chain blocks to each other establishing a chronological order of transaction.

- The miner with the longest chain of blocks establishes the state of the blockchain. (Longest Chain Rule)

Transmission Delays and Spontaneous Forking

- With perfect connectivity, Nakamoto consensus allows miners to coordinate without conflicts.

  That is, they all agree on the same state at all times.

  Thus, each miner stores the same chain of blocks.

Transmission Delays and Spontaneous Forking

- However, over the internet, connectivity is imperfect and miners are subject to transmission delays.

  So miners can temporarily have conflicting views on the state.

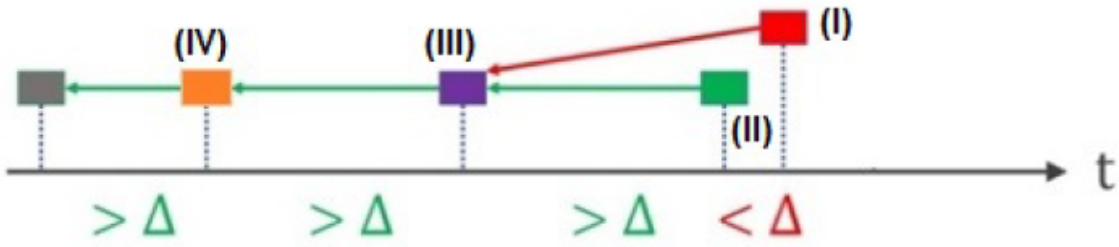
- In this case the blockchain forks: multiple children for a single parent block.

- Fork resolution: Select the first child block received.

  The other blocks are discarded (forked blocks).

Transmission Delays and Spontaneous Forking

- Transmission delay $\Delta > 0$:



The red block (I) is forked by the green block (II).

A fork originates at the purple block (III).

No fork at the orange block (IV).

Research Question

I analyze the implications of transmission delays at the consensus layer on blockchain design and welfare.

- First model to endogenize block size at consensus layer and inflation.

- General equilibrium model:

  Miners' economy (consensus)

  Users' economy (inspired by new monetarism)

  Protocol designer (social planner)

- Binary blocks for closed form solution.

  Extension with continuous block size. $\Longrightarrow$ calibration

Literature

- Market Microstructure models:

  Huberman et al. (2019).
  Easley et al. (2019).
  Hinzen, John, Saleh (2022).

  These cannot incorporate both endo block size and inflation.

- BFT-Style blockchains:

  Amoussou-Guenou et al. (2023).

- Tokenomics of Proof-of-Stake:

  John et al. (2021).
  Jermann (2023).

Findings

- Transaction (gas) fees:

  Inefficient policy tool to raise miner rewards from users.

  Discourage high value usage of the blockchain.

  Transmission delays $\Longrightarrow$ fees needed to incentivize miners to record transactions. (Recording Constraint)

- Seigniorage:
  Needed to reward miners when transaction load on the blockchain is low. (Activity Constraint)

  $\Longrightarrow$ Both fees and seigniorage needed to attract miners and secure the blockchain. (Participation Constraint)

Findings

- Block rate:

  Transmission delay limit the maximum block rate

  $\Longrightarrow$ Limited scalability problem.

- Uncle block rewards:

  Mitigate the limited scalability problem.

- Token burning (in progress):

  Incentive for miners to verify blocks of their predecessors.

Recording Incentives

- Assume M homogenous miners.
- Each miner produces μ/M blocks per unit of time (Poisson process).
- Blocks can be empty $a = 0$ or contain one transaction $a = 1$.
- Expected payoff for proposing a block with size $a \in \{0, 1\}$:

$$R_a(m_0, M) = z(\pi, \tau) P_a(m_0, M) (\pi + a\tau),$$

Recording Incentives

- Assume M homogenous miners.
- Each miner produces μ/M blocks per unit of time (Poisson process).
- Blocks can be empty $a = 0$ or contain one transaction $a = 1$.
- Expected payoff for proposing a block with size $a \in \{0, 1\}$:

$$R_a(m_0, M) = z(\pi, \tau) P_a(m_0, M) (\pi + a\tau),$$

$m_0 = \#$**other** miners choosing $a = 0$.

$P_a(m_0, M) =$ probability of updating the consensus chain.

$\pi =$ seigniorage (inflation rate).

$\tau =$ transaction fee rate.

Recording Incentives

- Win probabilities:

$$P_a(m_0, M) = \mathbb{P}\left(T_m + a\Delta < \min\left\{T_0, T_1 + \Delta\right\}\right).$$

- Likelihood ratio:

$$L(m_0, M) \equiv \frac{P_0(m_0, M)}{P_1(m_0, M)}.$$

- Incentive compatibility ($a = 1$ vs $a = 0$):

$$\frac{\tau}{\pi} \geq L(0, M) - 1 = (M - 1)(1 - e^{-\mu\Delta/M}). \qquad \text{(RC)}$$

RC becomes more stringent with faster block production and a longer transmission delay.

Recording Incentives

- Normal form game of block size (2 Miners):

Miner 1 \ Miner 2	$a = 0$		$a = 1$	
$a = 0$	$\frac{1}{2} z\,\pi$	$\frac{1}{2} z\,\pi$	$P_0 z\,\pi$	$P_1 z\,(\pi + \tau)$
$a = 1$	$P_1 z\,(\pi + \tau)$	$P_0 z\,\pi$	$\frac{1}{2} z(\pi + \tau)$	$\frac{1}{2} z(\pi + \tau)$

$$P_0 > \frac{1}{2} > P_1$$

Miner Activity

- Assume that miners produce full blocks when possible and face a flow energy cost c per unit of time.

- Let Q denote the number of pending transactions (mempool size).

- Positive profit flow requires:

$$\pi_0 = \frac{\mu}{M} z(\pi, \tau)\pi - c \geq 0 \qquad \text{for } Q = 0, \qquad \text{(AC)}$$

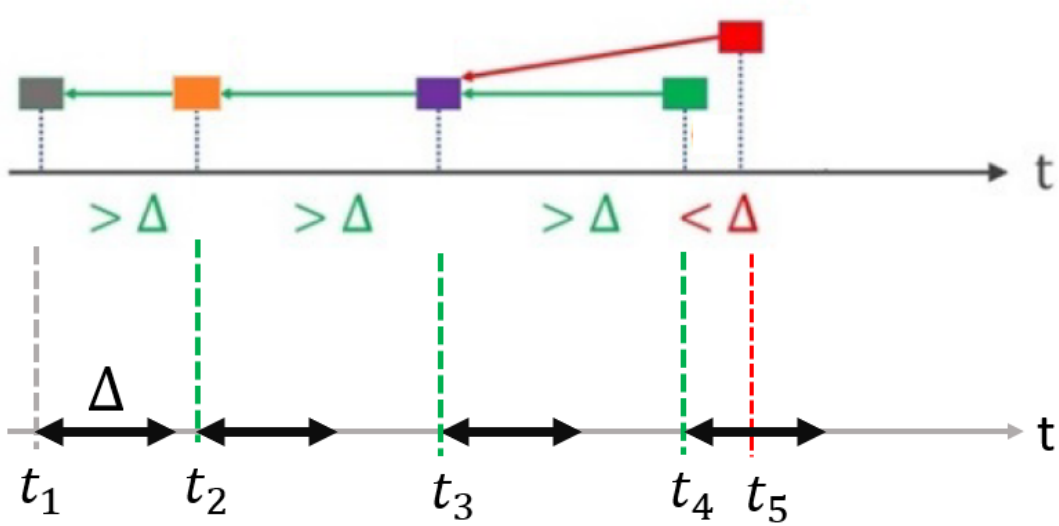
$$\pi_1 = \frac{\mu e^{-\mu\Delta}}{M} z(\pi, \tau)\,(\pi + \tau) - c \geq 0 \qquad \text{for } Q \geq 1.$$

$\implies$ $\pi > 0$ necessary for activity.

Fork Probability

$$\pi_1 = \frac{\mu e^{-\mu\Delta}}{M} z(\pi,\tau)\,(\pi+\tau) - c \geq 0 \qquad \text{for } Q \geq 1.$$

- $e^{-\mu\Delta}$ is the probability that a block is forked by its predecessor.



$$e^{-\mu\Delta} = \mathbb{P}(t_B - t_{B-1} < \Delta)$$

- $\lambda := \mu e^{-\mu\Delta}$ = blockchain growth rate.

Miner Lifetime Utility

- Discounted profits at rate r net of entry cost F:

$$V^m = \frac{\mathbb{E}_0(\pi_t)}{r} - F.$$

- Expected profit flow $\rho := \mathbb{P}(Q \geq 1) = \alpha/\lambda$:

$$\mathbb{E}_0(\pi_t) = \rho\pi_1 + (1-\rho)\pi_0 = \frac{z(\pi,\tau)\left[\lambda\pi + \alpha\tau\right]}{M} - c.$$

- Participation under free-entry:

$$M = \frac{z(\pi,\tau)\left[\lambda\pi + \alpha\tau\right]}{c + rF} \geq \underline{M} \qquad \text{(PC)}$$

Blockchain Users and Welfare

- Welfare combines user surplus (Web3 buyers and sellers) and miner surplus.

$$W = \max_{\pi,\tau,\mu} \quad V^b + V^s + MV^m \qquad \text{subject to } W \geq 0$$

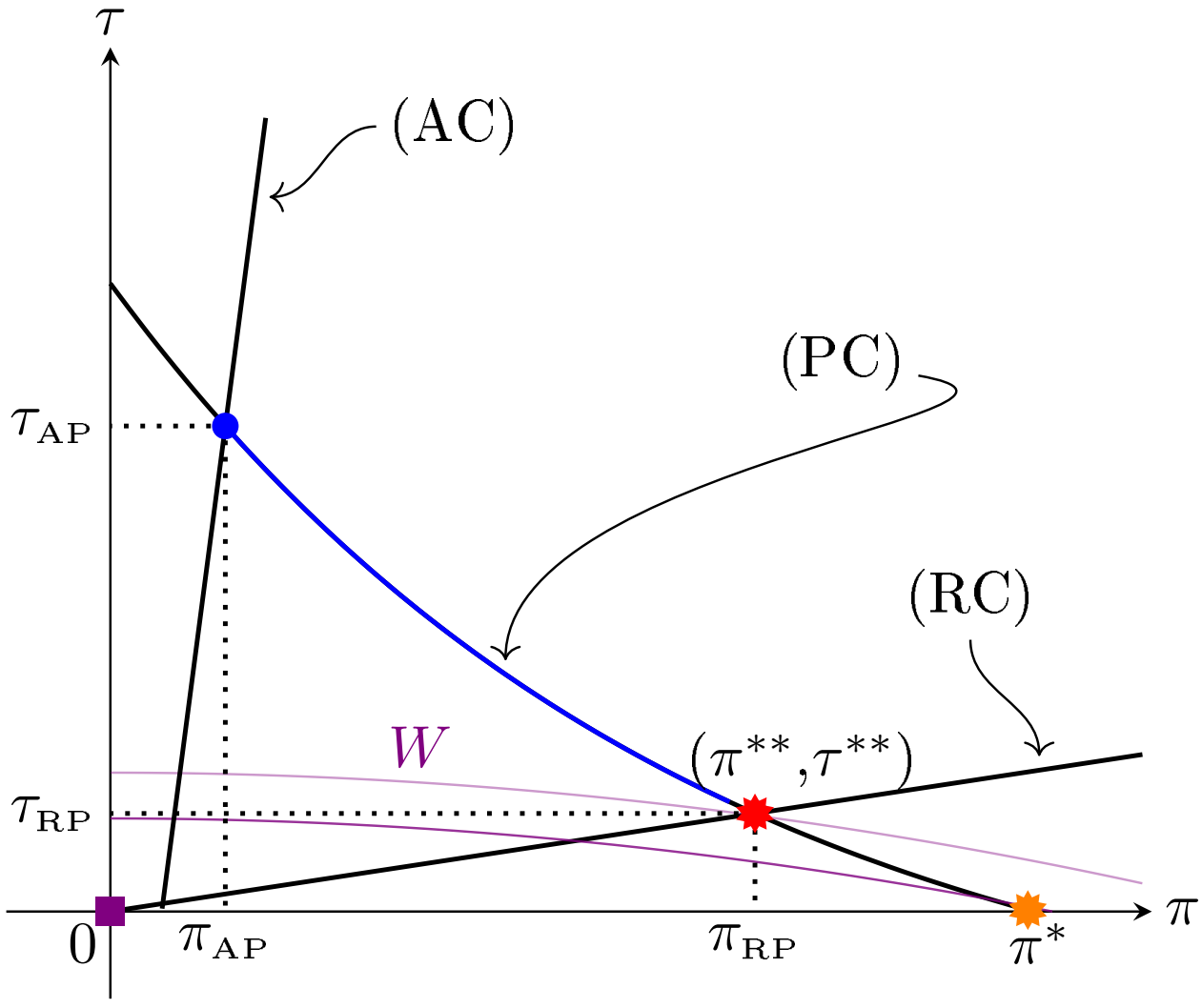
- Buyers make TIOLI offer to sellers:

$$y(\pi,\tau) = z(\pi,\tau)\beta(\rho)(1-\tau).$$

- Welfare = Trade surplus - liquidity costs - blockchain costs:

$$W = \max_{\pi,\tau,\mu} \quad \frac{\alpha}{r}\left(u\left(y(\pi,\tau)\right) - \frac{y(\pi,\tau)}{\beta(\rho)}\right) - \frac{y(\pi,\tau)}{\beta(\rho)(1-\tau)} - M\left(\frac{c}{r} + F\right).$$

Incentive-Compatible Welfare Maximization



$$\mu^* = \arg\max_{\mu} \beta(\alpha/\mu e^{-\mu\Delta}) = \arg\max_{\mu} \mu e^{-\mu\Delta} = 1/\Delta$$

Uncle Block Rewards

- Now design specifies also ϕ:

  $\phi =$ Seigniorage on forked blocks.

  Design parameters: $(\pi, \tau, \phi, \lambda)$:

- Expected payoff for proposing a block with size $a \in \{0, 1\}$:

$$R_a(m_0, M) = z(\pi, \tau, \phi) \left[P_a(m_0, M)\pi + a \left(\tau P_a(m_0, M) + \phi P_F(m_0, M) \right) \right].$$

$P_F(m_0, M) =$ Probability that the block is forked.

Uncle Block Rewards

- Incentive to play $a = 1$ now depends also on the probability ratio

$$X(m_0, M) \equiv \frac{P_F(m_0, M)}{P_1(m_0, M)} = \frac{M - m_0 - 1}{M} \left(1 - e^{-\mu\Delta/M}\right).$$

- Uncle block rewards relax the recording constraint:

$$\tau \geq \left[\pi \left(L(m_0, M) - 1\right) - \phi X\left(m_0, M\right)\right]$$

$$= (M-1)(1 - e^{-\mu\Delta/M})(\pi - \phi) \quad \text{for } m_0 = 0. \qquad \text{(RC')}$$

- Satisfied without fees ($\tau = 0$) for $\phi = \pi$.

- ϕ increases welfare by eliminating the recording-constraint.

Conclusion

- Study impact of transmission delays on blockchain consensus and usage.
- Explain need for transaction fees and limited scalability.
- In progress:

  Fee burning explained by consensus frictions (transmission delays + verification costs).

Thank you!