Getting Blockchain Incentives Right

Zahra Ebrahimi
CMU - Tepper

Bryan Routledge
CMU - Tepper

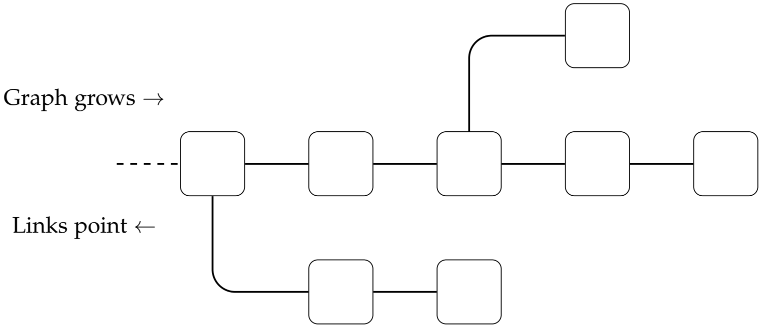
Ariel Zetlin-Jones
CMU - Tepper

October 2020

Blockchain

- Blockchain: "Technology" for decentralized, distributed ledger
- Key Features:
  - Ledger: ordered list of transactions
  - Distributed: users (miners) maintain own copy of the ledger
  - Decentralized: no centralized authority controls "correct" ledger
- How to secure public blockchains?
  - This paper: role of economic incentives
  - Develop new blockchain framework to study strategic agents' incentives

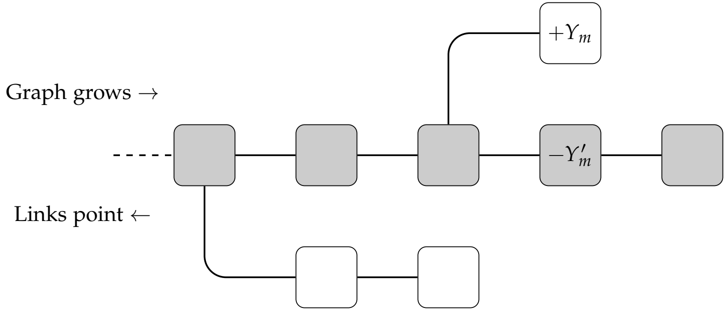
Blockchain Consensus, Forks, and Graphs



- Study miners' choice of *where* to add new data
- Existing research has shown longest chain may not be an equilibrium:
  - If any one miner has a lot of "power" or value of spent Bitcoins large
  - Then what is an equilibrium?
  - Need a richer model of miner's actions, payoffs, and strategies

Blockchain Consensus

- We develop framework to study consensus



- Will show consensus must prevent:
  - A <u>coordination</u> problem: Agent m deviates to put $+Y_m$ <u>on</u> consensus chain
  - A <u>double spend</u> problem: Agent m deviates to take $-Y'_m$ <u>off</u> consensus chain
- Our equilibrium protocol eliminates unintended incentives in existing protocols
  - Robust: valid equilibrium for arbitrary distribution of record keeping "power"

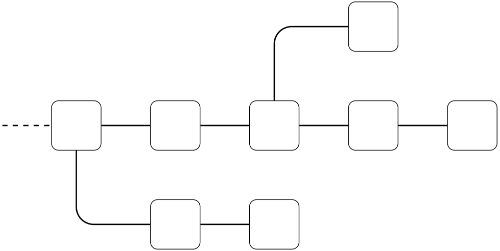
Environment

Ingredients

- M strategic agents (game among "miners")
- Represent blockchain ledger as a graph (tree)
- Agents choose *where* to add new data
- Today: interpret model as Bitcoin
- In paper: show how framework can generalize to other (public) blockchains (e.g. Ethereum) and other consensus "protocols"

Model Blockchain Structure

- Represent blockchain database as a graph (tree)



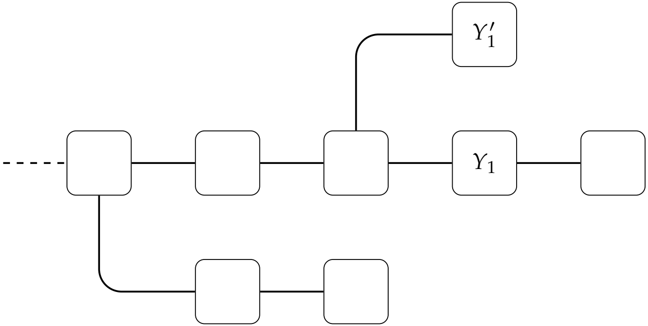
- $\mathcal{B}(G_t)$ is set of blocks (nodes) in graph G_t
- For any $b \in \mathcal{B}(G_t)$, $C(b, G_t)$ is chain of blocks to b
- Miner action: $a_{m,t} \in \mathcal{B}(G_t)$
- Miner m's block added with probability p_m

Blocks

- In each period $t = 0, 1, 2, \ldots$
  - New block b of "transactions"
  - List of credits and debits for each agent
    - $Y_{m,b}$: net credit for agent m in block b
    - $y_{m,b} = \bar{y}$ if agent m added block b (block reward)

$$\vec{Y}_b$$
$$\vec{y}_b$$

Preference for Consensus



- Net credits on chains others mine "worth more"
- If other miners choose middle, Y_1 worth more than Y_1'

Miners' Payoffs

- Date-t utility from a graph = "coins on the consensus chain"

$$U_m(\vec{a}, H_t) = (1-\delta) \sum_{b \in \mathcal{B}(G_t)} \left[\left(Y_{m,b} + y_{m,b} - \lambda Y_{m,b} \Delta \right) \frac{\sum_{i \neq m} p_i \mathbb{1}_{[b \in C(a_i, G_t)]}}{\sum_{i \neq m} p_i} \right]$$

  - Miners care about "balances"
  - Miners have direct preference for consensus
  - Miners care about offline (real) settlement
    - $\lambda = 1$ (indicator) when "goods delivered"'
    - Δ = scalar reflecting cost of delay

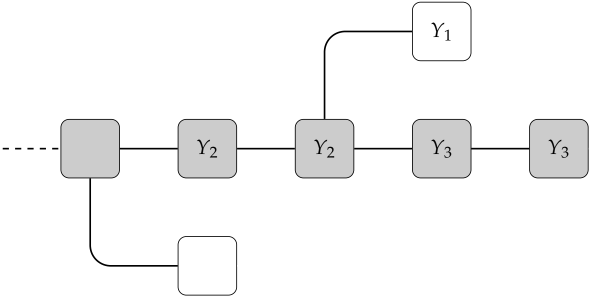
- Lifetime

$$(1-\delta)\mathbb{E}_0 \sum_t \delta^t \sum_{b \in \mathcal{B}(G_t)} \left[\left(Y_{m,b} + y_{m,b} - \lambda Y_{m,b} \Delta \right) \frac{\sum_{\{i \neq m : b \in C(a_{i,t}, G_t)\}} p_j}{\sum_{\{i \neq m\}} p_j} \right]$$

Consensus (Equilibrium) Protocols

Illustration I: Longest Chain is Not Public Perfect

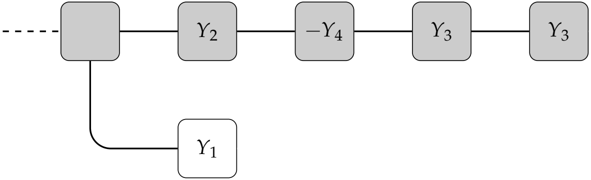
Longest chain induces coordination failure:



- Longest chain consensus = middle fork
  - On path, over next two periods, $m = 1$ expects $2p_1\bar{y}$
    (if $E[Y_1] = 0$ and $\delta \approx 1$)
  - If $m = 1$ tries deviates, expects $p_1^2\,[Y_1 + 2\bar{y}]$
    - Incentivizes $m = 1$ to deviate: if (Y_1 big relative to $\bar{y}$) or (p_1 big)
    - Big miners exploit consensus to acquire off-consensus chain value

Illustration II: Longest Chain is Not Public Perfect

Longest chain induces double spend problem:



- Suppose $m = 4$ has large negative transaction
- Once $m = 4$ receives “goods”, attempt to mine bottom fork
    - If successful, consensus changes, can spend Y_4 again
    - Folk wisdom: hard if p_4 “small”
        - Ignores economics: profitable deviation if Y_4 “large” (see Biais et al (2019); Budish (2019))

Checkpoints and Approval Weights

- Build equilibrium strategy using *checkpoints* and *approval weights*
  - Checkpoints, $\kappa_t(H_t)$: Determine settlement lag, resolve double spends
  - Approval weights: Coordination device
- Approval Weights of Terminal Blocks:
  - Add p_m to block weight if miner m has positive coin balance along chain beyond $\kappa_t(H_t)$
  - Function only of mining weights and transactions
- Checkpoints
  - $\kappa_{t+1}(H_{t+1}) =$ *parent* of "terminal" block ahead of $\kappa_t(H_t)$ with highest approval weight

Equilibrium Illustration in Simplified Game

- *Technical Condition 1 (strong):* For all H_t such that subgraph from $\kappa(H_t)$ has a fork, $Y_t = 0$.

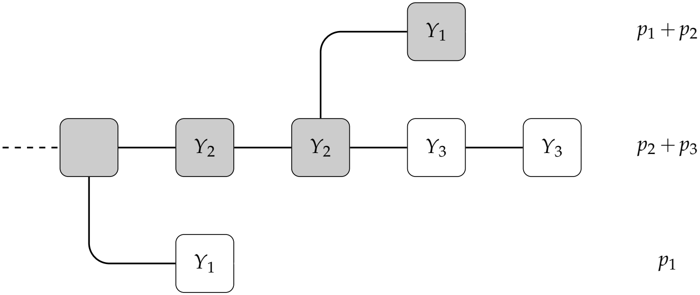
Proposition (Equilibrium in Restricted Game)

Under Technical Condition 1, there exists an equilibrium with no coordination problems and no double spending.

- Equilibrium strategy: Choose the block following the checkpoint with the highest approval weight
- Simple game illustrates role of checkpoints, approval weights
- Will show how to (arbitrarily) relax restriction

Resolving Coordination Failures with Approval Weights (Off Path)

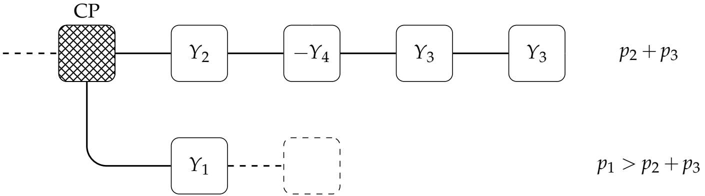
Approval weights disincentive coordination failures



- Construct approval weights for each fork
- If $p_1 > p_2 > p_3$, approval weighting selects top fork
  - Implication $m = 3$ alone cannot modify approval weight of middle fork

Resolving Double Spends with Checkpoints (Off Path)

History dependence disincentivizes double spending



- No in incentive to deviate from consensus before Y_4 settles
- Once Y_4 settles, adding block to bottom fork has no impact (behind checkpoint)
  - Highlights important link between online and offline strategies

Checkpoint Equilibrium

- *Technical Condition 2 (weak):* Fix $N \geqslant 1$. Suppose for all H_t such that $\kappa_{t-N}(H_{t-N}) = \cdots = \kappa_t(H_t)$, $Y_t = 0$.

Theorem (Checkpoint Equilibrium)

Under Technical Condition 2, there exists an equilibrium with no coordination problems and no double spending for all distributions of mining power, p.

- Implications and Limitations

  1. When $N > 1$, off-path strategies tolerate temporary lack of consensus
     - Speed of return to consensus depends on distribution of Y_t
  2. Settlement lag essential for eliminating double-spending
     - Suggests blockchain useful for large value transactions?
  3. Important link between latency and optimal settlement lag
     - Checkpoint subject to latency creates potential for lack of consensus

Conclusions

- Developed new economic framework to analyze blockchain consensus (equilibria)
- Consensus and permanence sensitive to equilibrium strategy
- Developed new consensus protocol using framework
  - History dependence
  - Settlement lags
- Framework allows for formalization of other protcols
  - Y_t represents value of software on the blockchain? (Ethereum)
  - Link mining power, p_m to past transactions? (Proof-of-stake)