An Axiomatic Approach to Bitcoin

Jacob Leshno and Philipp Strack

Chicago and Yale

December 9, 2019
Can we do more than building variations of Bitcoin? how?
What We Do:

- We propose a mechanism design approach to study decentralized protocols.

- **Basic idea:**
  ① Explicitly model the constraints imposed by decentralization and incentive compatibility requirements.
  ② Characterize all mechanisms compatible with these requirements.
  ③ Study the implications for the design of decentralized systems.

- **Main insight:**
  - Any decentralized proof-of-work protocol is “reward equivalent” to Bitcoin.
  - Results shown for Bitcoin and many others shown for Bitcoin apply to a wide range of protocols.
  - Potentially, promising approach for other situations.
Selection Rules

- There are \( n \geq 2 \) miners.
- Each miner contributes computational power \( x_i \geq 0 \) to the system.
- A selection rule \( p^n : \mathbb{R}_+^n \rightarrow \Delta^n \) specifies how miners are selected.
- \( p^n_i(x_1, \ldots, x_n) \) is the probability with which miner \( i \) mines the next block.
- Determines the miners incentives, to perform computations, join the network, etc.
- We assume that \( p^n_i(x_1, \ldots, x_n) \) is non-decreasing in \( x_i \).
Examples: Proportional Selection

- **Proportional selection** rule \( p^n_i(x) = \frac{x_i}{\sum_{j=1}^{n} x_j} \).

- Used in Bitcoin.

- Implementation:
  - The first miner who solves a “computational riddle”.
  - Apply SHA-256 hash function twice solution valid if small enough.
  - Best strategy try values at random.

- Many other potential implementations (e.g. min hash).

- Essentially systems engineering problem which we do not model.
Examples: Winner-Take-All Rule

- **Winner-Take All (WTA) rule**

\[
p^n_i(x) = \begin{cases} 
\frac{1}{|\arg\max_j x_j|} & \text{if } x_i \in \arg\max_j x_j \\
0 & \text{else}
\end{cases}
\]

- **Implementation:**
  - Abstracting away from network frictions.
  - Fix a time interval (10 minutes).
  - Miner who computed the most hashes mines the next block.
Comparison of Miner Behavior

- Different selection rules induce different miner behavior.
- Suppose miner $i$ has cost $c \cdot x_i$.
- Every miner values a block 1.
- Consider the game where miners chose $x_i$ to maximize

$$p_i^n(x) - c x_i.$$  

- WTA $\equiv$ complete information All-Pay auction

$$P[x_i \leq s] = n^{-1/2}s.$$  

- Proportional selection $\equiv$ Tullock contest.

$$x_i = \frac{n - 1}{n^2}.$$
A Mechanism Design Perspective

- Given that the selection rule determines miner behavior a natural agenda is:
  1. Find all \((p, x)\) that are “feasible” & “incentive compatible”.
  2. Find the best one according to some criterion.

- Parallel to the single good allocation/procurement problem:
  1. \(p\) is the allocation probability.
  2. \(x_i\) is the transfer of agent \(i\).

- **Main Difference:**
  Decentralization imposes additional non-standard IC constraints.

- We focus on step 1.

- Propose three requirements/axioms:
  1. Symmetry/Anonymity.
  2. Decentralization.
  3. Robustness to Sybil attacks.

- These axioms correspond to desirable properties discussed in the literature.
Axioms
Axiom (Anonymity)

A selection rule is anonymous if it is invariant under permutations, i.e. for every \( n \) and every permutation \( \pi : \mathbb{R}_+^n \rightarrow \mathbb{R}_+^n \) it satisfies \( \pi(p^n(x)) = p^n(\pi(x)) \).

- Captures the idea that the mechanism treats every participant the same.
- As analysis is on the block level this implicitly encodes history independence.
- Proof-of-Stake does not satisfy this requirement.
Axiom (Robustness to Sybil Attacks)

An selection rule is robust to Sybil attacks if for every \( x \in \mathbb{R}^n_+ \), \( i \in \mathbb{N} \) and every \( \Delta \in [0, x_i] \)

\[
p^n_i(x) \geq p^{n+1}_i(y) + p^{n+1}_{n+1}(y),
\]

where \( y = (x_1, \ldots, x_{i-1}, x_i - \Delta, x_{i+1}, \ldots, x_n, \Delta) \).

- Formalized an incentive constraint present in an environment with free entry an without verifyable identities.
- No particpant \( i \) wants to mimic a new entrant \( n + 1 \).
- Implicitly encodes a free entry condition.
- This axiom relates situations with \( n \) and \( n + 1 \) miners.
An random selection rule is robust to merging if for every $x \in \mathbb{R}_+^n$ and every $i,j \in N$

$$p^n_i(x) + p^n_j(x) \geq p^n_i(y) + p^n_j(y),$$

where $y = (x_1, \ldots, x_{i-1}, x_i + x_j, x_{i+1}, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$.

- Imposes a decentralization requirement.
- No two miners can merge and increase their joint winning probability.
- Avoids the system to be controlled by relatively few miners.
- Crucial for digital currencies: large miners compromise security.
Theorem (Characterization)

A random selection rule \( p \) is anonymous, robust to Sybil attacks, and robust to merging if and only if is the proportional selection rule

\[
p^n_i(x) = \frac{x_i}{\sum_{j=1}^{n} x_j}.
\]  

- Monotonicity is not necessary for this result if one restricts to \( x \in \mathbb{Q}^n_+ \).
- Every protocol induces a selection rule equivalent to Bitcoin.
- **Impossibility result:** without giving up on one of the properties one can not go beyond Bitcoin’s design.
- Similar result shown in Chen, Papadimitriou, and Roughgarden (2019).
Proof Idea

1. Show that the Axioms imply that each agent is indifferent between splitting her computations between herself and a new fake arrival and not splitting herself.

2. Consider the case where \( x \in \mathbb{Q}_+^n \). Split each agent into identical copies all having the same \( x_j \) without changing agent \( i \)'s winning probability.

3. Use symmetry to infer agent \( i \)'s winning probability as the number of copies she controls.

4. Proceed inductively agent by agent.

5. Use the monotonicity of \( p \) to go from \( \mathbb{Q} \) to \( \mathbb{R} \).
Risk-Aversion

- Suppose miners are risk-averse.
- In addition suppose miners can commit to transfers between each other.
- Suppose two miners $i$ and $j$ share the reward from a block proportionally whenever they win in proportion to $x_i, x_j$.
- This leaves each miner with the same expected reward, but a less risky distribution in second-order stochastic dominance.

Corollary

For every selection rule that satisfies Axiom 1-3 any two risk averse miners have a strict incentive to merge their computational contributions and share the reward from mining a block proportional to their respective contributions.

- Commitment to the proportional sharing rule is implemented in mining pools through the address of a block.
- Shows that there is a tension between risk-aversion and robustness to merging across all decentralized protocols satisfying our axioms.
- Is this characterization sharp in the sense that all axioms are necessary?
  1. $p^n(x) = (1/2, 1/2, 0, 0, \ldots)$ is robust to merging and Sybil attacks, but not anonymous.
  2. The winner-take-all selection rule is symmetric and robust to Sybil attacks, but not robust to merging.
  3. The rule $p^n(x) = (1/n, \ldots, 1/n)$ is symmetric and robust to merging, but not robust to Sybil attacks.

- The impossibility to implement rule 3 in an environment where agents can freely join is what motivated Nakamoto’s Bitcoin protocol.
Equilibrium Computations

- Any protocol which satisfies our axiom is equivalent to a proportional selection rule.
- Suppose agent $i$ has (potentially non-linear) cost $c(x_i)$ of performing computations.
- Resulting game is equivalent to a Tullock contest.
- Existing results imply a characterization of equilibrium behavior which characterizes winning probabilities:
- Can be used to determine how many and which miners are active in equilibrium, how unequal the winning probabilities are, etc.
- Follows similar approach previously proposed by Arnosti and Weinberg (2019) for Bitcoin.
Equilibrium Computations

1 Szidarovszky and Okuguchi (1997): Assume $c$ is differentiable, strictly convex. Let $\rho_i(s)$ the unique solution to the equation

$$s^2 c_i'(\rho_i(s)) = s - \rho_i(s)$$

if $sc_i'(0) < 1$ and set $\rho_i(s) = 0$. Set $s^*$ solve $s = \sum_{i=1}^{n} \rho_i(s)$. The computations performed by miner $i$ equal $\rho_i(s^*)$.

2 Hillman and Riley (1989): Assume that $c_i(x_i) = \beta_i x_i$ and let $m$ solve

$$m = \min \left\{ k: \beta_{k+1} \geq \frac{k}{k-1} \text{avg} (\beta_1, \ldots, \beta_k) \right\}$$

(2)

The total computational power of the system equals

$$s = \frac{m - 1}{m} \frac{1}{\text{avg} (\beta_1, \ldots, \beta_m)}$$

and the number of computations performed by miner $i$ is given by

$$x_i = \begin{cases} 0 & \text{if } i > m \\ s(1 - \beta_is) & \text{if } i \leq m \end{cases}$$

(3)
- For example consider two miners where miner 1’s cost is $\gamma$ times miner 2’s energy cost.
- Assume cost are linear (for example energy cost).
- In any protocol that is anonymous, robust to Sybil attacks and merging miner 1 wins with probability $\frac{1}{1+\gamma}$.
- Indicates that concentration of mining activity in low energy cost countries.
Conclusion

- Proposed a mechanism design approach to the design of decentralized protocols.

- We characterized all protocols that are decentralized in the sense that they are anonymous, robust to Sybil attacks and robust to merging.

- All these protocols are reward-equivalent to Bitcoin and centralize if miners are risk-averse.

- Potentially powerful approach with many open questions:
  1. Proof-of-stake, i.e. relaxing anonymity.
  2. Relaxing free entry condition to require “bonds”.
  3. Other interesting axioms, ideas?

- Only first step, potentially fruitful to identify “economically feasible” set.
Thank you!