On Some Results and Challenges in Cryptoeconomics

Tim Roughgarden

(a16z crypto & Columbia University)

Crypto Economics Security Conference (CESC)

November 1, 2022

Starting Point: Mechanism Design

Starting Point: Mechanism Design

0, 0	-1, 1	1, -1
1, -1	0, 0	-1, 1
-1, 1	1, -1	0, 0

Game theory: analyze strategic aspects of a given game.

- dominant strategies, Nash equilibria, etc.

Starting Point: Mechanism Design

0, 0	-1, 1	1, -1
1, -1	0, 0	-1, 1
-1, 1	1, -1	0, 0

Game theory: analyze strategic aspects of a given game.

- dominant strategies, Nash equilibria, etc.

Mechanism design: "inverse game theory" ("economist as engineer")

- identify desired outcome (e.g., welfare-maximizing allocation)
- design game w/that outcome as equilibrium (e.g., VCG mechanism)
  - payments allowed, traditionally in external currency (e.g., USD)

Starting Point: Mechanism Design

0, 0	-1, 1	1, -1
1, -1	0, 0	-1, 1
-1, 1	1, -1	0, 0

Game theory: analyze strategic aspects of a given game.

- dominant strategies, Nash equilibria, etc.

Mechanism design: "inverse game theory" ("economist as engineer")

- identify desired outcome (e.g., welfare-maximizing allocation)
- design game w/that outcome as equilibrium (e.g., VCG mechanism)
  - payments allowed, traditionally in external currency (e.g., USD)

Question: what if mechanism has access to a native currency?

Starting Point: Mechanism Design

0, 0	-1, 1	1, -1
1, -1	0, 0	-1, 1
-1, 1	1, -1	0, 0

Game theory: analyze strategic aspects of a given game.

- dominant strategies, Nash equilibria, etc.

Mechanism design: "inverse game theory" ("economist as engineer")

- identify desired outcome (e.g., welfare-maximizing allocation)
- design game w/that outcome as equilibrium (e.g., VCG mechanism)
  - payments allowed, traditionally in external currency (e.g., USD)

Question: what if mechanism has access to a native currency?

- *with power (minting/burning/etc.) comes responsibility (macro implications)*

Bitcoin as Mechanism Design

Desired outcome in Bitcoin/Nakamoto consensus:

- every node dutifully solves PoW puzzles, extends longest chain

Bitcoin as Mechanism Design

Desired outcome in Bitcoin/Nakamoto consensus:

- every node dutifully solves PoW puzzles, extends longest chain

Mechanism: for each block on longest chain, give reward to miner

- intuition: incentivizes miners to coordinate on longest chain

Bitcoin as Mechanism Design

Desired outcome in Bitcoin/Nakamoto consensus:

- every node dutifully solves PoW puzzles, extends longest chain

Mechanism: for each block on longest chain, give reward to miner

- intuition: incentivizes miners to coordinate on longest chain
- nuance [Eyal/Sirer 14]: can incentivize unintended behavior more!

Bitcoin as Mechanism Design

Desired outcome in Bitcoin/Nakamoto consensus:

- every node dutifully solves PoW puzzles, extends longest chain

Mechanism: for each block on longest chain, give reward to miner

- intuition: incentivizes miners to coordinate on longest chain
- nuance [Eyal/Sirer 14]: can incentivize unintended behavior more!

Question: where does the money for rewards come from?

Bitcoin as Mechanism Design

Desired outcome in Bitcoin/Nakamoto consensus:

- every node dutifully solves PoW puzzles, extends longest chain

Mechanism: for each block on longest chain, give reward to miner

- intuition: incentivizes miners to coordinate on longest chain
- nuance [Eyal/Sirer 14]: can incentivize unintended behavior more!

Question: where does the money for rewards come from?

- answer: newly minted coins (effectively, a tax on BTC holders)
- note: hard/impossible without control of a native currency

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

- consequence: given that Bitcoins never removed from circulating supply (i.e., no burning), block rewards must go to 0
  - miner rewards then come solely from transaction fees (and maybe MEV)

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

- consequence: given that Bitcoins never removed from circulating supply (i.e., no burning), block rewards must go to 0
  - miner rewards then come solely from transaction fees (and maybe MEV)
- obvious issue: if tx fees stay small, poor economic security

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

- consequence: given that Bitcoins never removed from circulating supply (i.e., no burning), block rewards must go to 0
  - miner rewards then come solely from transaction fees (and maybe MEV)
- obvious issue: if tx fees stay small, poor economic security
- subtle issue: unlike block rewards, tx fees vary widely across blocks
  - [Carlsten/Kalodner/Weinberg/Narayanan 16] miners incentivized to fork/replay blocks with unusually high tx fees, continually undercut each other

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

- consequence: given that Bitcoins never removed from circulating supply (i.e., no burning), block rewards must go to 0
  - miner rewards then come solely from transaction fees (and maybe MEV)
- obvious issue: if tx fees stay small, poor economic security
- subtle issue: unlike block rewards, tx fees vary widely across blocks
  - [Carlsten/Kalodner/Weinberg/Narayanan 16] miners incentivized to fork/replay blocks with unusually high tx fees, continually undercut each other
  - potential solution: smooth transaction fees over many of blocks

Micro Implications of Macro Decisions

Bitcoin's macroeconomic policy: hard cap of 21 million Bitcoins.

- consequence: given that Bitcoins never removed from circulating supply (i.e., no burning), block rewards must go to 0
  - miner rewards then come solely from transaction fees (and maybe MEV)
- obvious issue: if tx fees stay small, poor economic security
- subtle issue: unlike block rewards, tx fees vary widely across blocks
- modern version: MEV can vary widely across blocks
  - "MEV smoothing": smooth MEV payouts over validators
  - challenge: unlike tx fees, MEV not directly available to the L1 protocol

EIP-1559 as Mechanism Design

Desired outcome for (scarce) Ethereum blockspace: fully allocated, and allocated only to the most valuable transactions.

EIP-1559 as Mechanism Design

Desired outcome for (scarce) Ethereum blockspace: fully allocated, and allocated only to the most valuable transactions.

- aspiration: set tx fees = market-clearing price (supply = demand)

EIP-1559 as Mechanism Design

Desired outcome for (scarce) Ethereum blockspace: fully allocated, and allocated only to the most valuable transactions.

- aspiration: set tx fees = market-clearing price (supply = demand)
- first-price auction: let users figure out price for themselves

EIP-1559 as Mechanism Design

Desired outcome for (scarce) Ethereum blockspace: fully allocated, and allocated only to the most valuable transactions.

- aspiration: set tx fees = market-clearing price (supply = demand)
- first-price auction: let users figure out price for themselves
- EIP-1559: compute market-clearing price ("base fee") in-protocol

EIP-1559 as Mechanism Design

Desired outcome for (scarce) Ethereum blockspace: fully allocated, and allocated only to the most valuable transactions.

- aspiration: set tx fees = market-clearing price (supply = demand)
- first-price auction: let users figure out price for themselves
- EIP-1559: compute market-clearing price ("base fee") in-protocol
  - continually adjust (on-chain signal for excess demand = past block sizes)
  - bidding true valuation is optimal unless base fee << market-clearing price
  - non-manipulable by a block producer (even if colluding with end users)
  - twist: only works if base fee revenues directed away from block's producer!
    - see [Buterin 18], [Roughgarden 21] for details

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

EIP-1559's policy: burn them!

- note: only an option because of the native currency!

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

EIP-1559's policy: burn them!

- note: only an option because of the native currency!

Macroeconomic consequences: deflationary pressure on ETH.

- even more significant after post-Merge reduction in block rewards

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

EIP-1559's policy: burn them!

- note: only an option because of the native currency!

Macroeconomic consequences: deflationary pressure on ETH.

- even more significant after post-Merge reduction in block rewards

Question: is this a good thing?

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

EIP-1559's policy: burn them!

- note: only an option because of the native currency!

Macroeconomic consequences: deflationary pressure on ETH.

- even more significant after post-Merge reduction in block rewards

Question: is this a good thing?

- every ETH holder: yes! (cf., "ultra-sound money" meme)

Macro Implications of Micro Decisions

Question: to whom should base fee revenues be routed?

EIP-1559's policy: burn them!

- note: only an option because of the native currency!

Macroeconomic consequences: deflationary pressure on ETH.

- even more significant after post-Merge reduction in block rewards

Question: is this a good thing?

- every ETH holder: yes! (cf., "ultra-sound money" meme)
- every macroeconomist: no! (cf., 1990s Japan)

AMMs as Mechanism Design

Problem: enable the exchange of ETH (say) for USD and vice versa.

AMMs as Mechanism Design

Problem: enable the exchange of ETH (say) for USD and vice versa.

Traditional solution (NYSE, Coinbase, etc.): use an order book.

- issues: computationally costly, poor liquidity for long-tail tokens

AMMs as Mechanism Design

Problem: enable the exchange of ETH (say) for USD and vice versa.

Traditional solution (NYSE, Coinbase, etc.): use an order book.

- issues: computationally costly, poor liquidity for long-tail tokens

Automated market makers:"liquidity providers (LPs)" supply tokens

- market always willing to accept buy/sell orders at quoted price
- price determined by number of coins x,y of each type (e.g., y/x)

AMMs as Mechanism Design

Problem: enable the exchange of ETH (say) for USD and vice versa.

Traditional solution (NYSE, Coinbase, etc.): use an order book.

Automated market makers:"liquidity providers (LPs)" supply tokens

- market always willing to accept buy/sell orders at quoted price
- price determined by number of coins x,y of each type (e.g., y/x)

General problem: mechanism design with severe computational constraints (cf., algorithmic mechanism design [Nisan/Ronen 99]).

- note: not about cryptocurrencies per se (cf., lack of native token in Uniswap v1)

LVR in AMMs

AMM benefits: simplicity, guaranteed liquidity.

AMM costs: might force LPs to trade at worse-than-market prices.

- e.g., if AMM price is stale and corrected by an arbitrageur

LVR in AMMs

AMM benefits: simplicity, guaranteed liquidity.

AMM costs: might force LPs to trade at worse-than-market prices.

- e.g., if AMM price is stale and corrected by an arbitrageur

Question: how to measure these costs?

LVR in AMMs

AMM benefits: simplicity, guaranteed liquidity.

AMM costs: might force LPs to trade at worse-than-market prices.

- e.g., if AMM price is stale and corrected by an arbitrageur

Question: how to measure these costs?

Old answer: impermanent loss (IL).

- issue: adverse selection costs occluded by market movements

LVR in AMMs

AMM benefits: simplicity, guaranteed liquidity.

AMM costs: might force LPs to trade at worse-than-market prices.

- e.g., if AMM price is stale and corrected by an arbitrageur

Question: how to measure these costs?

Old answer: impermanent loss (IL).

- issue: adverse selection costs occluded by market movements

New answer: loss-versus-rebalancing (LVR).

- the "unhedgeable" component of IL
  - e.g., for "xy=k" curves: LP cost is $\sigma^2/8$

(see [Milionis/Moellemi/Roughgarden/Zhang 22] for details)

Grand Challenges (1 of 3)

Grand challenge #1: make macroeconomics our own.

- cf., game theory, mechanism design, etc.
  - issue: macroeconomics is already a minefield
- ex: is a hard cap “better” than permanent inflation?
- ex: are deflationary cryptocurrencies doomed?
- ex: what’s the “optimal” schedule for inflationary token rewards?
- ex: to what extent do such design decisions affect token price?

Grand Challenges (2 of 3)

Grand challenge #2: “optimal” L1 incentives.

- cf., optimal fault-tolerance in distributed computing
- ex: optimal economic security s.t. budget on costs to honest nodes
- ex: is slashing necessary (e.g., for optimal economic security)?
- ex: fundamental limits of in-protocol recovery from 51% attacks?
- ex: can liveness attacks be made as costly as consistency attacks?

Grand Challenges (3 of 3)

Grand challenge #3: interactions between layers of blockchain stack.

- ex: how to manage and incentivize P2P networks (“layer 0”)?
- ex: economics of (decentralized) layer-2s?
- ex: L1/L2 interactions
  - e.g., EIP-4844 and optimal multi-resource pricing
- ex: L1/application-layer interactions
  - e.g., is MEV unavoidable?
  - are inter-layer economic interactions inevitable in a decentralized system, or is the lack of clean separations an artifact of our current designs?

Grand Challenges (3 of 3)

Grand challenge #3: interactions between layers of blockchain stack.

- ex: how to manage and incentivize P2P networks ("layer 0")?
- ex: economics of (decentralized) layer-2s?
- ex: L1/L2 interactions
  - e.g., EIP-4844 and optimal multi-resource pricing
- ex: L1/application-layer interactions
  - e.g., is MEV unavoidable?
  - are inter-layer economic interactions inevitable in a decentralized system, or is the lack of clean separations an artifact of our current imagination?

THANKS!

FIN