



Introduction to Cryptoeconomics

Julian Ma

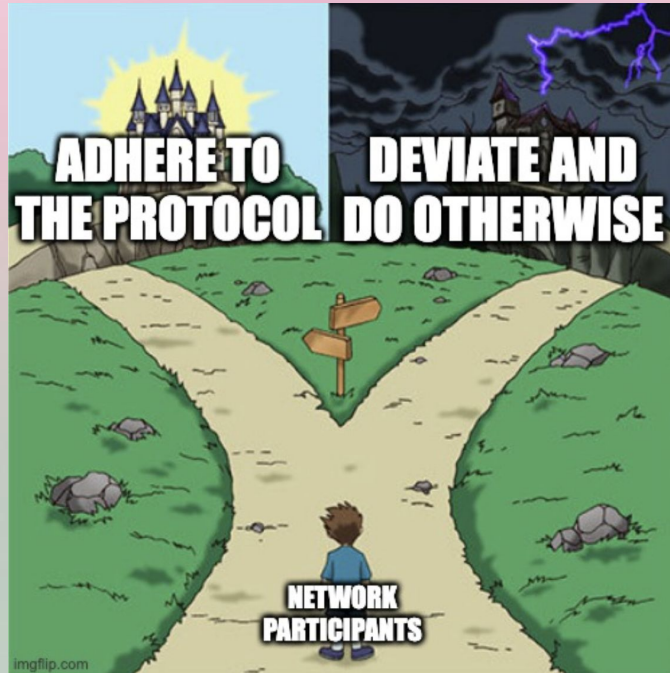
Robust Incentives Group, Ethereum Foundation



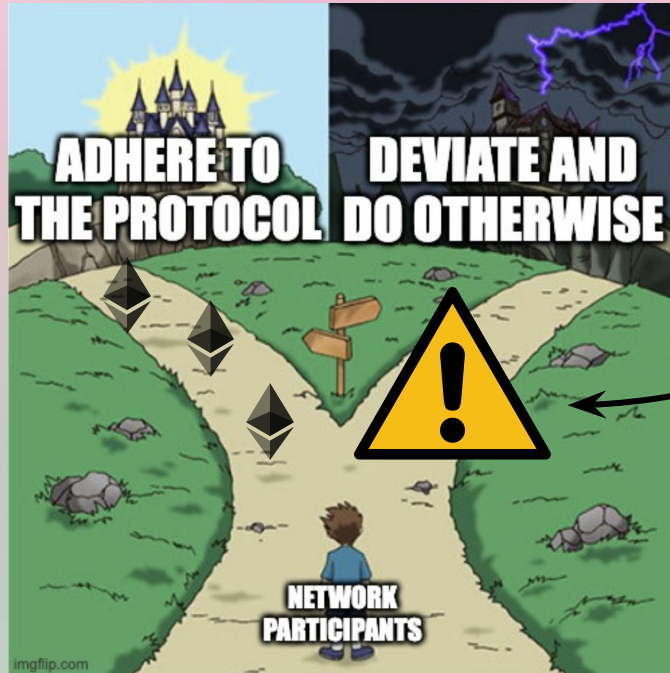
Section 1

What is Cryptoeconomics?

Economic incentives induce participants to do what the protocol wants them to do



Economic incentives induce participants to do what the protocol wants them to do

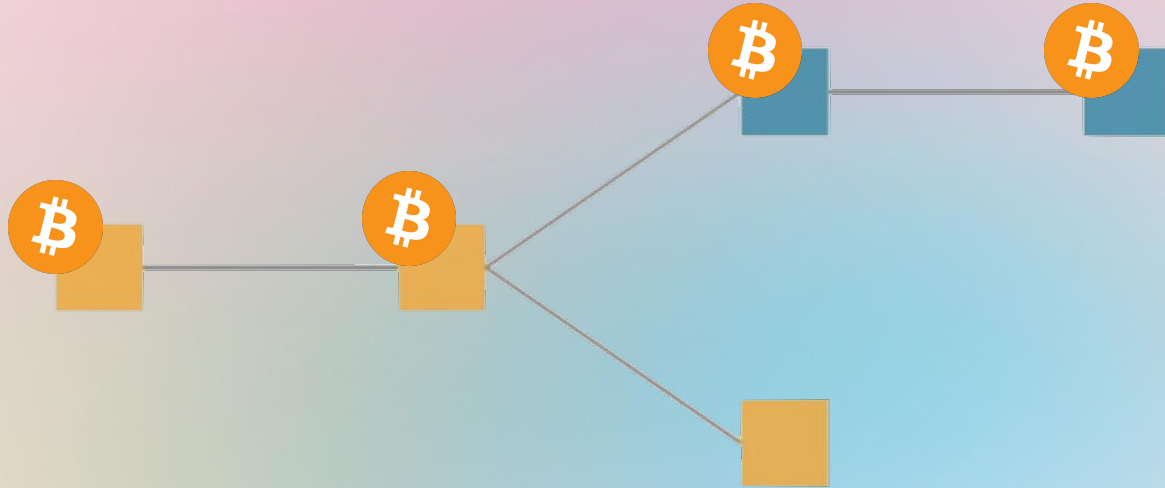


Cryptoeconomics

Game Theory

Study of **strategic behaviour**









“What should I do, given what other players will do”



Strategy of Miners

We usually represent games in tables.
What should the players do?







	Everyone else mines on Longest Chain	Everyone else mines on Other Chain
I mine on Longest Chain	 , 	 , 
I mine on Other Chain	 , 	 , 

Nash Equilibrium

No player has a **strict incentive to deviate**.

We reach an *equilibrium state*



	Everyone else mines on Longest Chain	Everyone else mines on Other Chain
I mine on Longest Chain		
I mine on Other Chain		

Mechanism Design

Study of the **design of strategic** situations (“reverse game theory”)

Left unchecked, many strategic situations have bad equilibria, or none.

How can we **design** the game (rewards, penalties, action spaces...) **so that good outcomes are reached?**



How do we design auctions efficiently?


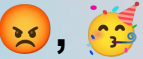

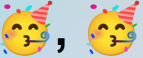
What does “efficient” mean?

Mechanism Design

We have multiple **Nash Equilibriums**

Incentivize such that the one we want becomes reality.



	Everyone else mines on Longest Chain	Everyone else mines on Other Chain
I mine on Longest Chain		
I mine on Other Chain		



Section 2

Gas Market

Market Overview (Pre EIP-1559)

Each **operation costs gas units**

Costs defined **relative** to other operations

Supply and demand determine **ETH per gas unit** users pay

Gas limit per block to preserve **decentralization**

Validators maximize pay-off by **including most valuable transactions** in a block

**ETHEREUM USERS
AFTER PAYING GAS FEES**

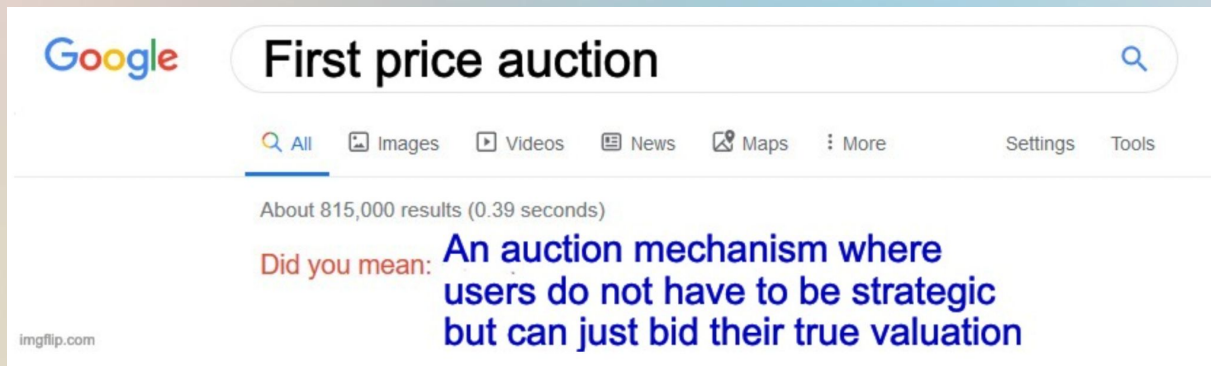


Blockspace Auction

This is a **first-price auction**: you pay what you bid if your bid wins

But... economists (*and game theorists*) don't like **first price auctions**!

What other options do we have?



Blockspace Auction

This is a **first-price auction**: you pay what you bid if your bid wins

But... economists (*and game theorists*) don't like **first price auctions**!

What other options do we have?

Second price auction: if you win the auction (post the highest bid), you pay the second-highest bid.



Dominant strategy incentive compatibility:

Your best strategy is to **bid your true value**

Others players should too, so... **Nash equilibrium!**

Example: winner bids 14 ETH but pays 10 ETH



**Why don't we have a second-price
auction for blockspace instead?**

Why we cannot have second-price auction

Miners choose transactions to maximize pay-off

Miners can also stuff blocks with **transactions to themselves!**

“Real” Block, Profit = 8

Fee	10	8	7	2
Revenue	2	2	2	2

Stuffed Block, Profit = 18



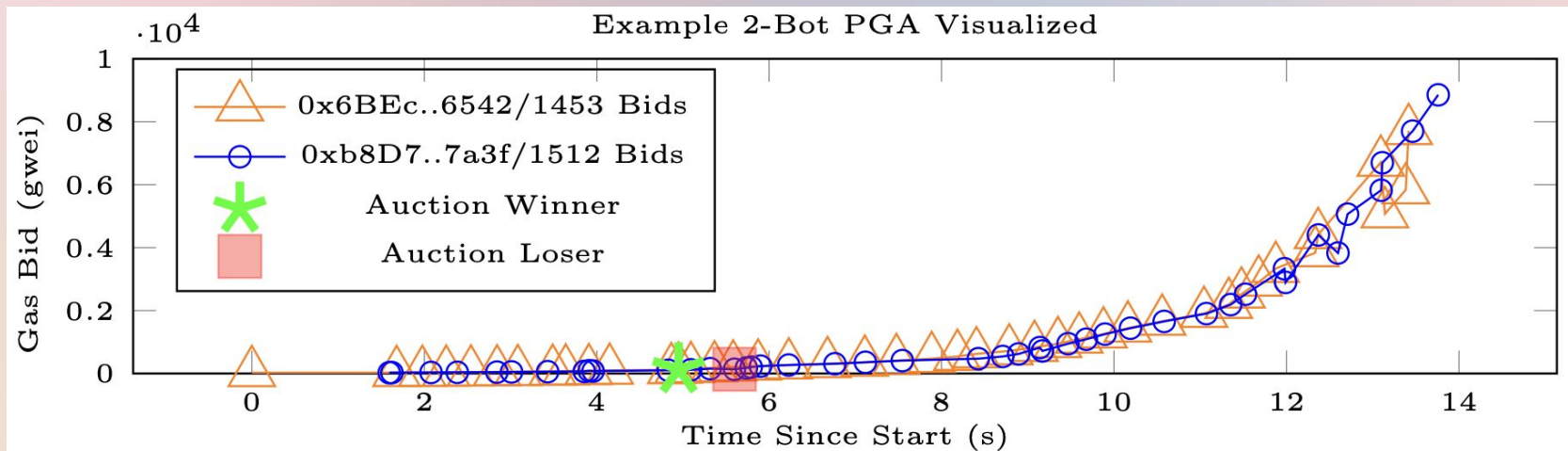
Fee	10	8	7	6
Revenue	6	6	6	6

Unique to cryptoeconomics: **adversarial environment**

Priority Gas Auction (PGA)

Consequence of the first-price auction: for valuable blockspace, fast bots continuously outbid each other.

Leads to congestion, wasted blockspace and higher gas fees



Source: [Flashboys 2.0](#)

EIP-1559: How the gas market changed

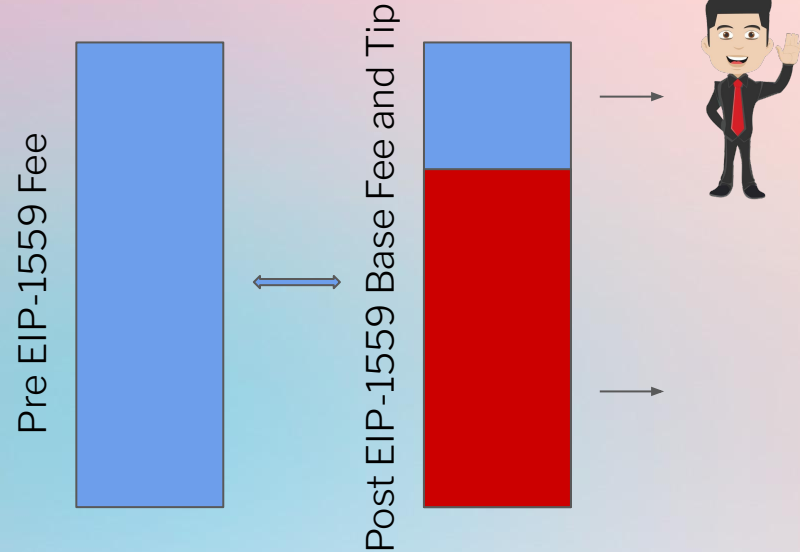
Up until now, talked about Pre EIP-1559

(Post EIP-1559) $\text{Fee} = \text{base fee} + \text{tip}$

Base fee depends on demand and supply and is set by the protocol

✨ **Incentive compatibility** ✨: users can bid their true value

Why does EIP-1559 not decrease fees?





Section 3

Maximum Extractable Value

Maximum Extractable Value

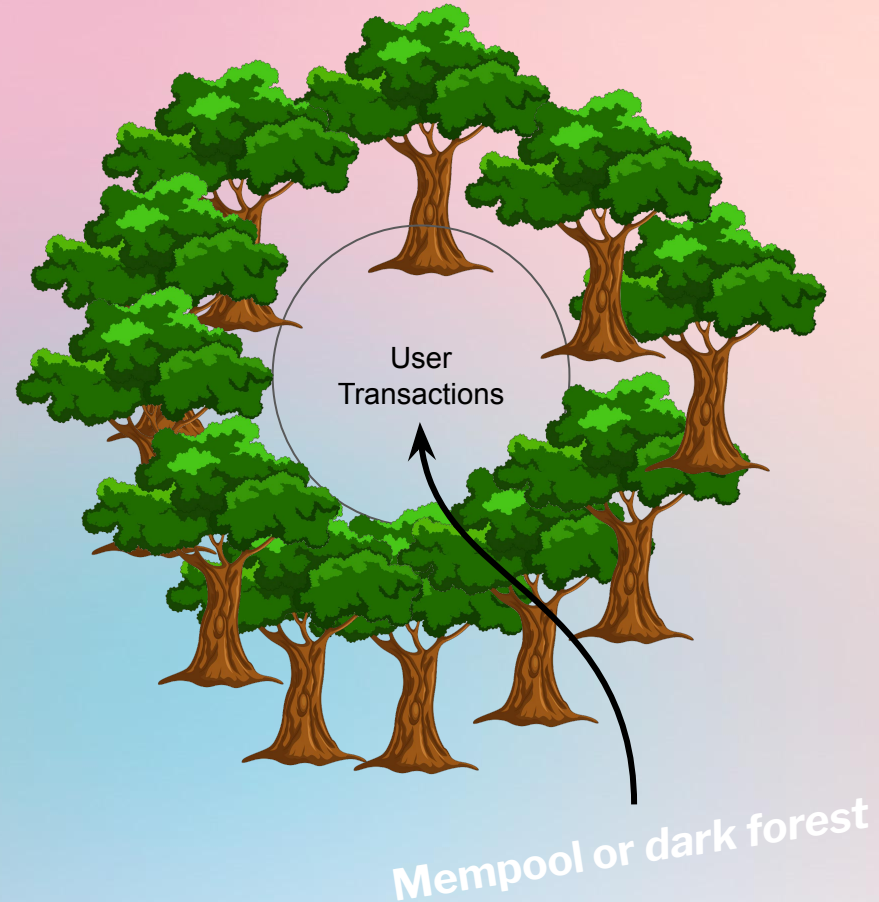
Users send their **transactions** to the **mempool**

Searchers look for **arbitrage** opportunities

Order of transactions can be manipulated

Some strategies are **risk-free** due to blockchain **atomicity**

Why not just “forbid” MEV?





MEV is bad

Searchers lead to **worst possible transaction execution**

MEV incentivizes **centralization**

Searchers waste blockspace

Smart MEV searchers could build other great projects

MEV is good

Searchers provide **valuable service** (backrunning, liquidations)

MEV can be **redistributed**

MEV needs to be extracted to ensure protocol **safety**



Conclusion MEV slide

Difficult to objectively say MEV is good or bad

Easy to say MEV cannot be ignored

Some responsibility for dApp developers: do not let your user's value be extracted

Responsibility for protocol: not all MEV can be mitigated via applications



Section 4

Ongoing Research

Ongoing research subjects

Robust Incentives Group (RIG) researches incentives in cryptoeconomic games

Maximum Extractable Value (MEV)

Multidimensional gas fees

Proposer Builder Separation (PBS)

Rollup Economics

Blockspace Derivatives

Foundation of cryptoeconomics: trustlessness, decentralization and game theory

Resources

Here are some links that may help you with delving deeper into cryptoeconomics

Name	What	Link
Robust Incentives Group (RIG)	Posts, papers & talks on cryptoeconomics	https://ethereum.github.io/rig
Flashbots	Posts focused on MEV and PBS	https://writings.flashbots.net/writings/
Ethresear.ch	Posts on general Ethereum focused research, including cryptoeconomics	https://ethresear.ch/
CryptoEconLab Protocol Labs	Posts, papers & talks on cryptoeconomics	CryptoEconLab Protocol Labs Research .

Personal blogs: [Barnabé](#), [Vitalik](#), [Pintail](#), [Tarun](#)

Thank you!

Strong research background?
Mechanism design expert?
Want to help us make sense of it?

Apply to the RIG now!



Barnabé Monnot, Julian Ma

Robust Incentives Group (RIG), Ethereum Foundation

barnabe@ethereum.org, julian.ma@ethereum.org



@barnabemonnot



@_julianma