Some ideas from economics and game theory (that are important for cryptoeconomics)

May 20, 2021

Outline

We will discuss a few key topics in today's learning session

- (Risk-Neutral) Asset Pricing
- Game Theory
- DeFi and the Oracle Problem

(Risk-Neutral) Asset Pricing

Question

Imagine if I were to offer to pay you $1 every day for the remainder of the year (225 days) if you gave me 7.5 UMA now.

Would you be willing to take this trade?

Question

Imagine if I were to offer to pay you $1 every day for the remainder of the year (225 days) if you gave me 7.5 UMA now.

Would you be willing to take this trade?

- How much is 7.5 UMA worth to you today?

Question

Imagine if I were to offer to pay you $1 every day for the remainder of the year (225 days) if you gave me 7.5 UMA now.

Would you be willing to take this trade?

- How much is 7.5 UMA worth to you today?
- How much is $1 per day worth to you today?

Present discounted values

Most people intuitively recognize that \$1 per day for 225 days is not worth \$225. How much is it worth?

We can compute the value of a sequence of payments by using a *present discounted value*.

If you could earn a return r on \$1 every day, then you'd have $(1 + r)$ tomorrow... In order to be willing to let me have a dollar today, I'd have to be willing to pay you $(1 + r)$ tomorrow or you would just keep your dollar.

Present discounted values

More generally, if someone promises you a sequence of payments $\{y_t\}_{t=0}^{T}$ then you should be willing to give them

$$X_t = \sum_{t=0}^{T} \left(\frac{1}{1+r}\right)^t y_t$$

In the crypto world, a "risk-free" return might be $r \approx 0.0002$ per day (7.5% APR), so if you valued your UMA at \$25 then we should have

$$187.5 \approx 7.5 \times 25 < \sum_{t=0}^{225} \left(\frac{1}{1+r}\right)^t \approx 220$$

Present discounted values and market capitalization

Game Theory (done right)

What is a game?

A game as defined by John von Neumann is

- A collection of players, $i \in \mathbb{I}$
- A set of actions for each player A_i
- A payoff function for each player that maps the action taken by each individual into that player's utility, $\pi_i : A_1 \times A_2 \times \cdots \times A_n \to \mathbb{R}$
- A timing protocol that specifies who gets to choose what when

What is a game?

A game as defined by John von Neumann is

- A collection of players, $i \in \mathbb{I}$
- A set of actions for each player A_i
- A payoff function for each player that maps the action taken by each individual into that player's utility, $\pi_i : A_1 \times A_2 \times \cdots \times A_n \to \mathbb{R}$
- A timing protocol that specifies who gets to choose what when

Warning: Either someone is going to take the game theory seriously or they won't. Someone can justify whatever they want using game theory if they aren't forced to formalize it. If they won't formalize it, call bullshit and tune out.

What is an equilibrium?

An equilibrium is defined as a strategy for each player s_i (either a single action or a probability distribution over actions) such that certain conditions are met.

Nash equilibrium

The most famous equilibrium concept that people have learned about in game theory is a “Nash equilibrium”

(Insert image from ”A beautiful mind” and describe how the movie got its title) A Nash equilibrium is a strategy for each player, $\{s_i\}$, such that the best response to everyone else’s strategy, s^{-i}, is s_i (the defined strategy for player i)

Prisoner's dilemma example

You can't talk about game theory without describing the prisoner's dilemma

		Player 2: Rat	Player 2: Silent
Player 1	Rat	$(-1, -1)$	$(4, -2)$
	Silent	$(-2, 4)$	$(3, 3)$

The only Nash equilibrium is (Rat, Rat) where the prisoner's turn on one another

Prisoner's dilemma cont'd

Is there a way to convince the prisoner's to cooperate?

1. Change the payoff structure (anyone who rats is punished more harshly than cops could punish)
2. Repeated game

Prisoner's dilemma cont'd

If we allow the players to play the prisoner's dilemma repeatedly (with the assumption that they discount the future at δ), then we can get cooperation. Why?

Prisoner's dilemma cont'd

If we allow the players to play the prisoner's dilemma repeatedly (with the assumption that they discount the future at δ), then we can get cooperation. Why?

Consider the following strategy for both players:

- Stay silent if your partner in crime has kept their mouth shut in the past, otherwise rat.

The payoff from continuing to cooperate is $\sum_{t=0}^{\infty} \delta^t 3$. The payoff from ratting becomes $4 + \sum_{t=1}^{\infty} \delta^t - 1$. Once can find a $0 < \delta < 1$ such that cooperation indefinitely is optimal.

Prisoner's dilemma cont'd

If we allow the players to play the prisoner's dilemma repeatedly (with the assumption that they discount the future at δ), then we can get cooperation. Why?

Consider the following strategy for both players:

- Stay silent if your partner in crime has kept their mouth shut in the past, otherwise rat.

The payoff from continuing to cooperate is $\sum_{t=0}^{\infty} \delta^t 3$. The payoff from ratting becomes $4 + \sum_{t=1}^{\infty} \delta^t - 1$. Once can find a $0 < \delta < 1$ such that cooperation indefinitely is optimal. **The takeaway is that the future can be a powerful tool.**

“Voting” game

Consider a town of 100 people that is choosing which digital currency to coordinate on. They have chosen to hold a vote on which currency to use and can either choose BTC or ETH.

Suppose that 75 people in the town prefer ETH and 25 people in the town prefer BTC. Your payoff is 1 if your preferred currency is chosen and 0 otherwise. What’s the Nash equilibrium?

“Voting” game

Consider a town of 100 people that is choosing which digital currency to coordinate on. They have chosen to hold a vote on which currency to use and can either choose BTC or ETH.

Suppose that 75 people in the town prefer ETH and 25 people in the town prefer BTC. Your payoff is 1 if your preferred currency is chosen and 0 otherwise. What’s the Nash equilibrium?

One Nash equilibrium is the 75 people who prefer ETH vote for ETH and the 25 people who prefer BTC vote for BTC. ETH is chosen and the town uses ETH

“Voting” game

Consider a town of 100 people that is choosing which digital currency to coordinate on. They have chosen to hold a vote on which currency to use and can either choose BTC or ETH.

Suppose that 75 people in the town prefer ETH and 25 people in the town prefer BTC. Your payoff is 1 if your preferred currency is chosen and 0 otherwise. What’s the Nash equilibrium?

Unforunately, this is not the only Nash equilibrium. The following is also a Nash equilibrium, all 100 people vote for BTC and the town uses BTC as its currency. No single individual’s deviation from this strategy has an effect on the outcome so it satisfies the best response criteria.

“Voting” game

Consider a town of 100 people that is choosing which digital currency to coordinate on. They have chosen to hold a vote on which currency to use and can either choose BTC or ETH.

Suppose that 75 people in the town prefer ETH and 25 people in the town prefer BTC. Your payoff is 1 if your preferred currency is chosen and 0 otherwise. What’s the Nash equilibrium?

This logic basically results in being able to support (almost) whatever you want as a Nash equilibrium in this game.

Trembling hand perfect equilibrium

The second NE of our voting game doesn't seem to fit with common sense. Can we come up with an equilibrium concept that eliminates it (while keeping the sensible one)?

Trembling hand equilibrium is a concept where we consider a perturbed game, Γ_ε. In this perturbed game, individuals are only allowed to play mixed strategies and must play each action with at least probability ε. A Nash equilibrium is a trembling hand perfect equilibrium if the Nash equilibrium is a Nash equilibrium in the sequence of perturbed games generated by $\lim_{\varepsilon \to 0} \Gamma_\varepsilon$

Revisiting the voting game

Consider a town of 100 people that is choosing which digital currency to coordinate on. They have chosen to hold a vote on which currency to use and can either choose BTC or ETH.

Suppose that 75 people in the town prefer ETH and 25 people in the town prefer BTC. Your payoff is 1 if your preferred currency is chosen and 0 otherwise.

There were many Nash equilibria and we wanted to know whether we could find an equilibrium concept that eliminated some of the unexpected equilibria (equlibria that resulted in BTC being the town's currency).

Revisiting the voting game

Let $\varepsilon > 0$. Consider the strategies $s_i = (1 - \varepsilon, \varepsilon)$, i.e. vote for BTC with probability $(1 - \varepsilon)$ and for ETH with probability ε then is this a best response strategy for someone who prefers ETH?

The individual's payoff is given by

$$u_i = \text{P}(>50 \text{ people vote for BTC}) \times 0 + >50 \text{ people vote for ETH}) \times 1$$

The individual can now have an effect on the probability that 51+ people vote for BTC/ETH because it won't just be 0 or 1. This means that they'll vote for their preferred currency.

The Oracle Problem

The oracle problem

In DeFi, the oracle problem deals with how to (reliably/truthfully) bring data that does not exist on the blockchain into the blockchain

For example, a synthetic blockchain asset that settles based on the price of gold needs to know the price of gold, but this data isn't native to the blockchain...How do we get it there?

The dependability/reliability of this oracle is crucial in DeFi due to a future in which the community can envision trillions of assets being secured by such an oracle.

Corruptible oracle

If an oracle could be corrupted, the attacker could make off with blockchain assets valued at millions (or even billions) of USD.

While it would be great if we could rely on DeFi participants to be honest, we have already seen elaborate attacks used to manipulate DeFi markets and abscond with hundreds of millions of USD, so it's crucial to build a hardened system that takes the risk of manipulation seriously.

Cryptoeconomic security for the oracle problem

Cryptoeconomic security involves designing systems that are secured by economic incentives.

In the case of the oracle problem (in DeFi) this means that one needs to design a system such that the cost of corrupting the system is higher than profit one earns via corruption.

The best way to then analyze whether this system achieves its goals is to analyze it via game theory or other economic tools.

Two approaches to the oracle problem

Here are two approaches that have been taken to the oracle problem has been approached in two main ways:

- Autonomous system that relies on participants to run "data nodes". These data nodes retrieve data from online sources and are then paid for uploading this data by requestors. If a submission is disputed then appeal to another layer of data nodes.
- Optimistic system that relies on DeFi participants to request/upload prices on their own, but secured by a system of bots that look for discrepancies. In the case of a discrepancy, turn to a vote system where holders of the token specify what the price should have been.

Security in the autonomous system

Consider a system that relies on N separate nodes to produce a price that is used to secure Ω (in USD) of DeFi assets. The data nodes are required to stake an amount d in order to submit a price and the system promises to pay x for each price that the data nodes provide.

What would it cost to corrupt the oracle (aka, bribe the N nodes)?

Security in the autonomous system

What would it cost to corrupt the oracle (aka, bribe the N nodes)?

If the nodes expect to the system to last indefinitely, expect to be chosen to submit each price with probability p, and discount the future at r then the present discounted value of their future earnings is

$$\gamma \equiv \sum_{t=0}^{T} \left(\frac{1}{1+r}\right)^{t} px = \frac{px}{r}$$

Security in the autonomous system

What would it cost to corrupt the oracle (aka, bribe the N nodes)?

If the nodes expect to the system to last indefinitely, expect to be chosen to submit each price with probability p, and discount the future at r then the present discounted value of their future earnings is

$$\gamma \equiv \sum_{t=0}^{T} \left(\frac{1}{1+r} \right)^t px = \frac{px}{r}$$

The system is then economically secure so long as $X < N\gamma$

Security in the optimistic system

Now consider an optimistic system that relies on individuals to submit their own prices (possibly through an automated bot of their own) with a stake d. Individuals who submit a price that is not disputed are rewarded with x. Any single person can choose to dispute the proposed price submitted by the submitter by disputing (possibly through an automated bot) and posting their own stake of d.

If a dispute is posted, all individuals who hold the oracle's token are asked to participate in a vote on what the price should have been. If they choose to vote on the "incorrect" price, we assume that the oracle has been corrupted and the token value drops to 0

What would it cost to corrupt the system?

Security in the optimistic system

What would it cost to corrupt the system?

It would require an individual to either not have a dispute filed against them or to corrupt 51% of the token holders. This gives us explicit bounds on the profit from corruption and the cost of corruption.

UMA's view on the history/future of financial contracts

1. *The jungle*: I want your asset so I take it
2. *"Government backed" financial contracts*: We enter into agreements and governments help enforce these agreements (sometimes at gunpoint)
3. *"Decentralized" oracles 1.0*: Individuals won't report false prices because they won't be able to collect their future payments.
4. *Optimistic decentralized oracles*: System is secured via economic incentives by explicitly ensuring that it's more expensive to corrupt the system than one could earn in profits by doing so

UMA builds with the optimistic decentralized oracles that we believe are the future of financial contracts.