A Primer to Game Theory & Incentivized Mechanism Design for Miners

Personal Background

- Found out about Bitcoin day after it launched - original mailing list
- GPU, FPGA, ASIC mining as early as 2010
- Experienced and seen every major scam
- Drop some truth bombs this presentation
- About Certus One
  - Cosmo's Game of Stakes Winners (#1 across all 6 categories)
  - Validator for a few networks and oracles.
  - We work with a lot of funds and institutions to help them through the process of staking.
  - We play at Defcon's Capture the Flag annually (7th this past year)

Certus.One

Core Human Incentives

- There are generally two groups of people that are involved in Crypto
  - Speculators (95% in my opinion)
  - Philosophical (5%)
- Understanding and designing different systems/incentives
- At its core, majority of humans are driven by greed
- Crypto economic systems become very similar to real world case scenarios given time
  - Wealth becomes concentrated in the top 1%
  - Building and sustaining a vibrant community - create the right incentives

Certus.One

Examples of Mechanisms

- Perks & Incentives (STX App Mining)
- Burning & Decay
- Staking, Inflation and hybrid rewards (like blockstack)
- Insurance Pools / Slashing Pools
- Penalties and Edge Cases
- Inter-blockchain communication (IBC) / Interoperability
- Foundation Economics / Grants
- Governance

Certus.One

Monetary Flow

- Understand how capital flows in and out of your ecosystem
- Take advantage (absorb) liquidity/capital/utility from other systems
  - Instead of depending on buyers of your token, take advantage of products/services from other projects/chains
- Retention vs acquisition
- How users will adapt (or revolt) to changes in economic policy

Certus.One

In the Beginning – PoW

- Quick Background
  - Cypherpunks
  - Very early days
  - Piratat40, Bitcoin savings & trust, Bitcoinica
- Even very early on, it was driven by greed/speculation
- Satoshi's decentralized economic design intended to give small players a chance to participate
- It was quickly gamed with the invention of FPGA and ASIC

Certus.One

Traditional Hardware Mining Game

- Mining hardware evolution
  - CPU to GPU to FPGA to ASIC
  - Tale of failures - Butterfly labs, KNC miner, CoinTerra, etc
  - It's an unfair playing field - heavily favored towards China
  - As a result, it's a race for fastest/most efficient chip and electricity/infrastructure cost
  - Story about TSMC
  - Mining with customer hardware then selling when its unprofitable
    - Why sell a miner for $5,000, when it can generate $3,000 per month?

Certus.One

PoW Groups

- Mining is dominated by 4 groups
  - Chinese Miner/Manufacture
  - Foreign governments
  - VC / Investor backed companies
  - Mom & Pop, self funded miners
- Different incentives for each group
  - Profit / Power
  - Currency Controls / Laundering
  - Seeking extreme profitability / speculation
  - Profit (few enthusiasts sprinkled in)
- Think / observe their interactions

Certus.One

Hardware Cartel

- Bitcoin mining hardware is essentially a cartel
  - There are no manufacturers of this hardware outside of China: the majority is owned by TSMC and a small portion by Global Foundries
  - Free/low cost electricity in China and government subsidies at scale
    - Ex. Government built a mining company their own hydroelectric dam with free/negligible cost for facilities
    - No environmental regulations, no building codes, worker safety, etc
    - Money laundering / foreign reserves. Convert Yuan, Iranian Rial to US - subsidized
- Mining has very low barrier of entry, does not require "highly intelligent and skilled workers"
- Thus, the Bitcoin Protocol primary incentives are a race to the bottom. The only exception is foreign governments - whose primary incentive is avoiding currency controls and/or bolstering foreign reserves

Certus.One

New form of Miners – PoS / Token Sales

- New Groups
  - Large Investors (VC) instead of Manufacturers/Miners
  - Largely focused on a single region because they were shut out the asian markets
  - Generally unfair ICO / sale structures - huge/no cap on investment and sybil attacks
  - Almost entirely speculators
  - Small groups of highly concentrated token holders - lacks community
- Different incentive mechanisms than PoW
  - Staking early yields larger rewards (higher inflation generally)
  - Thus, the HODL factor yield has a higher expected return than PoW

Certus.One

DeFi Mechanisms - Yield Farming

- DeFi is a pot of cash that runs in circles trying to maximize/manufacture returns - textbook financial engineering
- YAM, YFI, CRV, Spaghetti, YFV farming created new, interesting incentive structures and many iterations are being built upon it
- Example: a protocol with a token that governs a DeFi liquidity aggregation pool that holds tokens that generate yield by providing liquidity to a liquidity exchange, governing a lending protocol, and staking across 5 different assets (one of which is STX)
- How will the monetary flow in the above example? Where will the capital and users flock to?

Certus.One

Goals and Design

- **There is no perfect incentive design**
- Identify and create economic systems that are tailored to each specific stakeholder group
  - Token distribution strategy
- Long term focused but with short term incentives
- Account for edge cases and understanding monetary flow
- Structure governance to be able to adapt and modify if needed
- Assume everyone is incredibly intelligent and will game your systems to the extreme

Certus.One

Thank you! Q&A

Learn more at **Certus.One**

Richard@Certus.one

Follow me on Twitter: @Megatron

TheRichardLi.com